POLITIETS ADGANG TIL TRAFIKKDATA OG IDENTIFIKASJONSDATA FRA TILBYDERE AV EN ELEKTRONISK KOMMUNIKASJONSTJENESTE

Universitetet i Oslo
Det juridiske fakultet

Kandidatnummer: 554

Leveringsfrist: 25. november 2010

Til sammen 17 990 ord

24.11.2010

Innholdsfortegnelse

1 INNLEDNING

1.1 Bakgrunn og problemstilling

For 10 til 15 år siden var mobiltelefoner og høyhastighetsinternett nærmest en kuriositet, noe man bare hadde tilgang til om man vandret i de rette kretsene eller hadde en viktig nok jobb til at det kostbare utstyret og tjenestene ble påkostet av arbeidsgiver. I dag er den teknologiske hverdagen en helt annen. I 2009 fantes det over 5,4 mobiltelefonabonnenter i Norge[1] og over 4,2 millioner av oss hadde pr. juni 2010 tilgang til internett gjennom enten ISDN, bredbånd eller ADSL oppkobling.[2]

Den nye teknologien og utbredelsen av den har naturlig nok ført med seg nye og mer teknologiske hjelpemidler for politiet i sin kriminalitetsbekjempelse. To av de viktigste av disse hjelpemidlene er trafikkdata og identifikasjonsdata.[3]

Et raskt tilbakeblikk på noen av de mest profilerte sakene i media det siste året viser at trafikkdata og identifikasjonsdata er blitt et viktig hjelpemiddel for politiet under sin etterforsking. Da Lars Flem Andreasen ble drept på Kongsvinger tidlig i 2009 bare 18-år

[1] Post- og Teletilsynets rapport om "Det norske ekommarkedet" s. 7

[2] Internet Usage Statistics, www.internetworldstats.com

[3] Begrepene er definert nærmere under kapittel 3 og 4.

gammel, var en av de viktigste grunnene til at politiet fant den skyldige drapsmannen at han bare for en kort periode hadde brukt den dreptes mobiltelefon etter drapet.[4]

I en annen profilert sak fra 2009 ble et høytstående gjengmedlem drep i sin bil på Haugerud i Oslo. Etterforskingen tydet på at drapet var bestilt og planlagt gjennom en fiktiv Facebook-profil på internett. Ved hjelp av trafikkdata og identifikasjonsdata tilknyttet bestemte IP-adresser, kunne politiet her få indikasjoner på hvem som var innblandet i drapssaken og hvem som bestilte og utførte drapet.[5]

At trafikkdata er blitt et meget viktig hjelpemiddel for politiet i en etterforskingssituasjon ser vi også ved et utvalg av statistikker fra de største kommunikasjonstilbyderne på markedet; Telenor og NetCom, samt ved å se på fritaksoversikten fra Post- og Teletilsynet (PT). Sistnevnte opplyser at de i nærmere 2000 saker i fjor opphevet tilbyders taushetsplikt etter anmodning fra politiet. Telenor kan opplyse om at de i 2009 mottok 2453 anmodninger fra politiet om å få utlevert lokasjonsdata. Det samme året mottok NetCom 1730 henvendelser fra politiet om å få utlevert trafikkdata.

Med bakgrunn i den enorme teknologiske utviklingen som har skjedd på dette området over forholdsvis kort tid, vil en av problemstillingene i avhandlingen være hvordan lovverket som omhandler utlevering av trafikkdata og identifikasjonsdata har utviklet seg i takt med den teknologiske utviklingen, og hva som har vært bakgrunnen for disse endringene. Hovedproblemstillingen i avhandlingen vil derimot redegjøre for dagens rettstilstand på området og hvordan lovverket virker sett i forhold til våre viktigste rettssikkerhetsprinsipper og hensyn, men også i forhold til politiets rolle som kriminalitetsbekjemper. Avslutningsvis vil avhandlingen kort belyse fremtidige utfordringer i forhold til kriminalitetsutviklingen og utviklingslinjene vedrørende trafikkdata i andre land.

---

[4] http://www.glomdalen.no/nyheter/article5120932.ece

[5] http://www.tv2nyhetene.no/innenriks/krim/mener-gjengbroedre-bestilte-drap-paa-facebook-3070741.html

1.2 Avgrensning

Avhandlingen retter seg mot trafikkdata og identifikasjonsdata som lagres hos en tjenestetilbyder av en elektronisk kommunikasjonstjeneste. Avhandlingen legger her til grunn samme begrepsbruk som fremkommer i lov om elektronisk kommunikasjon av 4. juli 2003 nr. 83, heretter ekoml.

Etter ekoml. § 1-5 nr. 4 er elektronisk kommunikasjonstjeneste en: *"tjeneste som helt eller i det vesentligste omfatter formidling av elektronisk kommunikasjon og som normalt ytes mot vederlag."*

Elektronisk kommunikasjon er etter § 1-5 nr. 1 definert som: *"overføring av lyd, tekst, bilder eller andre data ved hjelp av elektromagnetiske signal i fritt rom eller kabel i et system for signaltransport."*

En "tilbyder" blir i samme bestemmelse nr. 14 definert som *"enhver fysisk eller juridisk person som tilbyr andre tilgang til et elektronisk kommunikasjonsnett eller –tjeneste."*

At avhandlingen kun omhandler trafikkdata og identifikasjonsdata avgrenser automatisk mot innholdet i kommunikasjonen. Med innhold menes for eksempel hva som blir sagt i en telefonsamtale, hva som blir skrevet i en e-post, en SMS eller lignende. I tillegg avgrenser oppgavens tema mot informasjon som politiet selv innhenter ved bruk av hjelpmidler som teknisk sporing eller kommunikasjonskontroll etter for eksempel lov om rettergangsmåten i straffesaker av 22. mai 1981 nr. 25 (strpl.) § 216a.

Avhandlingen retter seg mot beslag og utlevering av trafikkdata, samt utlevering av identifikasjonsdata som politiet foretar som ledd i etterforsking. Hvordan disse sporene blir brukt som bevis under for eksempel hovedforhandlinger eller hvordan og til hvilken grad tilbyderne lagrer denne informasjonen vil nevnes kort, men vil ikke bli problematisert inngående.

1.3 Rettskildebruk

Avhandlingen legger til grunn alminnelig juridisk metode i det følgende, og problemstillingene i avhandlingen besvares på bakgrunn av de rettskildeprinsipper og faktorer som gjelder for norsk rett. De juridiske spørsmål og problemstillinger vil i all hovedsak løses med hjelp av formell lov, forskrifter, forarbeider, etterarbeider og rettspraksis. Også juridisk teori og reelle hensyn vil bli brukt som rettskildemoment hvor de nevnte rettskildene er uklare eller gir et sprikende tolkningsresultat.

I tillegg til norsk rett, vil avhandlingen også berøre områder for internasjonal rett, da hovedsakelig gjennom tolkning av Den Europeiske Menneskerettighetskonvensjonen av 1950, heretter EMK. Konvensjons- og domstolspraksis vedrørende EMK må derfor også nevnes som relevant rettskilde i avhandlingen.

2 VIKTIGE HENSYN VED UTLEVERING AV TRAFIKKDATA OG IDENTIFIKASJONSDATA

2.1 Innledning

Med ”hensyn” menes de forskjellige rettsikkerhetsprinsipper og rettslige hensyn som politiet, retten, tilbyder og PT må vurdere når trafikkdata og identifikasjonsdata skal utleveres, enten ved hjelp av ekoml. § 2-9 tredje ledd, ved frivillig utlevering, eller etter reglene i strpl. § 203, jfr. 205, § 210 eller § 216b. Da de undernevnte prinsippene og hensynene vil ligge som et ”teppe” over lovverket og komme inn som avveiningsmomenter ved bruk av de aller fleste lovbestemmelsene som hjemler slik utlevering ser jeg det som hensiktsmessig å nevne disse kort innledningsvis.

2.2 Hensynet til effektiv kriminalitetsbekjempelse

Det samfunnsmessige hensynet som påhviler politiet i deres oppgaver med å løse straffbare handlinger vil være et meget tungveiende vurderingsmoment ved bruk av bestemmelser som hjemler inngrep i borgernes rettsfære. Bakgrunnen for dette hensynet er politiets rolle som kriminalitetsbekjemper. Denne rollen skaper en samfunnssikkerhet og trygghet for borgerne, samt allmenn tillitt til myndighetene som straffeforfølger de som begår kriminelle handlinger. At politiet får et visst ”spillerom” under etterforskingen og et effektivt lovverk til å bekjempe kriminalitet vil også virke avskrekkende for de som vurderer å begå kriminelle handlinger.

2.3 Kontradiksjonshensynet

Hensynets tradisjonelle mening innebærer at partene som er innblandet i en sak som går, eller skal gå for rettssystemet, varsles om rettsmøter, får være til stede under forhandlingene, og får gjøre seg kjent med materialet som er innhentet, samt å ta til motmæle mot dette. Hensynet kommer bl.a. frem av strpl. § 232, jfr. § 92.

Prinsippet er også forankret i bestemmelsen om rettferdig rettergang i EMK art. 6. At også kravet til rettferdig rettergang omfatter et krav om kontradiksjon er uomtvistet og kommer frem av bl.a. to dommer i EMD mot Norge.[6]

Prinsippet vil også komme inn som moment i etterforskingssituasjon ved at den mistenkte, eventuelt andre som berøres av utleveringen eller beslaget, gis underretning om dette. Flere lovbestemmelser i strpl. unntar fra prinsippet ved å gi muligheter for utsatt underretning, se bl.a. strpl. §§ 208a og 210a. Hensynet bak slike bestemmelser er åpenbart for at politiet skal kunne utføre en så god og effektiv etterforsking som mulig. Denne adgangen setter press på prinsippet som rettssikkerhetsprinsipp og bruk av utsatt underretning krever derfor ofte at straffverdigheten på det som blir foretatt av den mistenkte er av slik alvorlig art at prinsippet derfor må vike.

2.4 Hensynet til den personlige sfære

Dette hensynet innebærer at myndighetene må ta visse forholdsregler før man foretar inngrep i det som kalles borgernes personlige eller private sfære. Den private sfære ble av Ytringsfrihetskommisjonen i NOU 1999: 27 gitt følgende definisjon:

> *"Den private sfære, eller intimsfæren, er sfæren der man omgås med dem man kjenner som personer. Den er, og bør være, en frihetssfære i den forstand at den i omfattende grad er beskyttet mot reguleringer og inngrep fra det offentlige."*[7]

Den personlige sfæren forstås som et vidt begrep og omfatter personlige integritet, autonomi og privatlivets fred. I dette ligger det også et krav om at den enkelte har oversikt over informasjonen som lagres om en selv og hvordan denne brukes.[8] Dette kravet blir i stor grad avhjulpet gjennom underretningsplikten tilhørende de forskjellige

---

[6] Se Botten vs. Norway (1996) og Walston vs. Norway (2003)

[7] NOU 1999:27 s. 28

[8] Se ekomloven § 2-7 annet ledd, siste punktum.

straffeprosessuelle tvangsmidlene, men som nevnt over vil underretningsplikten ofte måtte vike for hensynet til en effektiv etterforsking.

Med tanke på at trafikkdata er taushetsbelagt informasjon etter ekoml. § 2-9 første ledd, samt at lagring av slike data faller inn under virkeområdet til lov om behandling av personopplysninger av 14. april 2000 nr. 31 (persl.) § 3 a, jfr. § 2 nr 1 og 2, tilsier at trafikkdata faller inn under det som regnes for å være den enkeltes ”personlige sfære.”

Et av problemene med dette hensynet er å vite hvor langt begrepet ”den personlige sfære” skal forstås. En kjennelse i Borgarting Lagmannsrett inntatt i RG. 2006 s. 811 gir et illustrerende eksempel på hvor grensen kan gå. Etter et attentatforsøk begjærte politiet utlevert all teletrafikk som hadde vært innom en basestasjon lokalisert i et bysentrum i en periode på over fem dager. Begjæringen ble ikke godtatt av retten da utlevering av slike opplysninger ville *”krenke personvernet til en svært stor krets av personer som har krav på hemmelighold om sine bevegelser og sin mobiltelefoni.”* Kjennelsen ble avsagt under dissens (2-1) hvor den dissenterende dommer var uenig i flertallet og mener at politiet burde ha krav på slike opplysninger begrunnet i hensynet til effektiv etterforsking.

2.5 Forholdsmessighetsprinsippet – Strpl. § 170a

Bruk av alle tvangsmidler i straffeprosessloven må vurderes etter forholdsmessighetsprinsippet som er lovfestet i strpl. § 170a. Prinsippet verner den enkelte mot at tvangsmiddelet ikke blir et ”uforholdsmessig inngrep.” Det skal da legges vekt på ”sakens art” og ”forholdene ellers”, jfr. § 170a annet punktum. Ved beslutning om beslag eller utleveringspålegg av trafikkdata vil man da blant annet måtte ta hensyn til fordelene politiet oppnår ved utlevering sett i forhold til den personvernskrenkelse mistenkte eller andre som omfattes av utleveringen utsettes for.

Prinsippet gjelder uavhengig av om det er domstolen, politiet eller påtalemyndigheten som treffer beslutningen[9] og vil komme inn som vurderingsmoment ved alle ledd i utleverings- eller beslagsbestemmelsene, også på hvor lenge et tvangsmiddel skal brukes, eventuelt om det er hensiktsmessig å bruke tvangsmiddelet for hele den gitte fristen.[10]

Bestemmelsen er en såkalt minimumsregel, og flere lovbestemmelser i straffeloven stiller opp strengere krav enn hva som kan leses ut av § 170a, se bl.a. strpl. § 216c som krever at etterforskingsmetoden skal være av "vesentlig betydning" for å oppklare saken.

Prinsippet gjelder som nevnt for alle typer tvangsmidler politiet har adgang til å bruke, men får økt styrke når tvangsmiddelet er av særlig inngripende karakter, jfr. bl.a. strpl. §§ 200a annet ledd og 216c første ledd.

Da prinsippet er meget viktig i straffeprosessen vil det bli mer inngående forklart og eksemplifisert i teksten hvor dette faller naturlig.

2.6 Legalitetsprinsippet

Et sentralt og viktig element i det materielle rettsikkerhetsbegrepet er legalitetsprinsippet. Prinsippet antas å ha grunnlovs rang i kraft av konstitusjonell sedvanerett.[11] Tradisjonelt er begrepet forstått slik at myndighetene ikke kan gripe inn i borgernes rettsfære uten hjemmel i formell lov eller gjennom forskrift gitt i formell lov. Avhandlingen vil legge denne tradisjonelle forståelsen av begrepet til grunn for den videre drøftelsen.

Prinsippet er kommet til uttrykk i Grunnloven gjennom § 96 første alternativ som lyder "ingen kan dømmes uden efter lov". Selv om dette kravet gjelder på strafferettens område

---

[9] NOU 2009:15 punkt 7.6

[10] Ot.prp.nr. 64 (1998-1999) s. 146

[11] Knoph s. 725

vil de samme kravene i stor grad også gjelde på straffeprosessens område,[12] noe som støttes av de mer straffeprosessuelle grunnlovsbestemmelsene i § 99 som verner mot fengsling og § 102 som verner mot vilkårlige husundersøkelser.

Prinsippet gir også visse kvalitetskrav til lovregler som hjemler inngrep fra myndighetenes side. Tunge inngrep i den enkeltes rettsfære, slik som husransakelse og skjult overvåking, krever klar og uttrykkelig hjemmel i lov. De mindre og mer beskjedene inngrepene krever ikke like sterk lovhjemmel, og kan for eksempel følge av forarbeider eller instruks. Hvor denne grensen går kan være uklart, og må vurderes konkret i hvert enkelt tilfelle.

Kravet til klarhet blir særlig begrunnet i forutberegnlighet i lovverket. Forutberegnligheten innebærer at borgerne lett kan forholde seg til lovverket og gjøre seg kjent med dette. Av den grunn skal man derfor være forsiktige med å tolke bestemmelser som hjemler inngrep i borgernes private sfære utvidende eller analogisk.

Om prinsippet også verner mot psykiske inngrep i den personlige sfære er et åpent spørsmål. Tradisjonelt sett har prinsippet ikke vernet slike interesser, men med tanke på økt fokus i samfunnet på rettssikkerhet og menneskerettigheter de siste årene må dette synet sies å ha fått mer slagkraft. Hopsnes hevder blant annet at dersom det offentliges samlede kontroll med individet blir stor ”kan dette tale for å utvide legalitetsprinsippets forbudsnorm av hensyn til frihet som verdi.”[13]

Utvalget i NOU 2004:6 som hadde som mandat å gjennomgå det gjeldene regelverket for hvilke metoder politiet kunne bruke seg av i forebyggende øyemed og hvordan disse sto seg sett opp mot regelverket som gjaldt for personvern var av den oppfatning at

[12] NOU 2009:15 s. 28

[13] Hopsnes (2005) s. 95

legalitetsprinsippets materielle skranke også gjelder for politiets handlinger, men hvor grensene her går er vanskelig å trekke.[14]

Det er viktig å nevne at prinsippet ikke er i veien for politiets alminnelige handlefrihet.[15] I dette ligger det en adgang for politiet til å spane på personer eller steder hvor det mistenkes at det foregår ulovlig virksomhet, infiltrere kriminelle miljøer eller samle inn informasjon som er tilgjengelig for offentligheten. Først når disse tiltakene blir så intensive og inngrepene i den personlige sfære blir så store krever legalitetsprinsippet hjemmel i lov, men som departementet uttaler i Ot.prp.nr. 64 (1998-1999) så skal det "mye til".[16]

Kravet til klarhet i lovverket ble drøftet av Høyesteretts ankeutvalg i en kjennelse inntatt i Rt. 2009 s. 394. Politiet hadde her fremsatt en begjæring om kommunikasjonskontroll etter strpl. § 216b. Telefonen var registrert på en annen person enn den som politiet nå antok disponerte over den, og ville bringe identiteten på disponenten på det rene da han var mistenkt for til dels grov narkotikavirksomhet. Ankeutvalget la vekt på at verken ordlyden i § 216b eller forarbeidene til bestemmelsen tilsier at punktene a - d ikke er ment å være uttømmende. Utvalget så heller ingen åpninger i bestemmelsen for bruke den til å identifisere den mistenkte. Ankeutvalget så at lovgiver nok ville inkludert slike tilfeller i bestemmelsen om de hadde vært oppmerksomme på problemstillingen, men at kravet til klar lovhjemmel må få sterkt tilslag ved bruk av slike metoder fra politiets side. Dette synet ble av Høyesterett hovedsakelig begrunnet i legalitetsprinsippet og lovkravet som stilles opp i EMK art. 8.

[14] Se bl.a. s. 64 og s. 89

[15] Ot.prp.nr.64 (1998-1999) s. 16

[16] Ibid. s. 17

2.6 Nødvendighetsprinsippet

Dette prinsippet kommer blant annet til uttrykk i lov om politiet av 4. august 1995 nr. 53 (politil.) § 6 annet ledd, og vil si at offentlige myndigheter ikke skal gripe inn overfor borgerne i større omfang og med sterkere midler enn det som er nødvendig for å realisere hjemmelsgrunnlagets formål. Et viktig element under denne vurderingen er om det som handlingen søker å oppnå kan nås på en annen og mindre inngripende måte. Behovet for inngrepet avhenger av krenkelsens art, retning og omfang, derunder risiko og skadegrad.[17]

2.7 EMK - Artikkel 8

2.7.1 Innledning

Da den europeiske menneskerettighetskonvensjonen (EMK) ble vedtatt av Europarådet den 4. november 1950 ble noen av de mest grunnleggende menneskerettighetene, herunder retten til liv, vern mot tortur, rett til ytringsfrihet og vern om privatlivet, gitt en sentral plass i den internasjonale lovverksstrukturen.

Norge tiltrådte konvensjonen 15. Januar 1952, men den ble ikke inkorporert i det norske lovverket før ved lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven) av 21. mai 1999 nr. 30. Lovens § 3 gir blant annet konvensjonen forrang ved motstrid mellom andre bestemmelser. At den stillings er styrket i norsk rett Kommer også til uttrykk i grunnloven § 110c som pålegger statens myndigheter å sørge for at menneskerettighetene i den nasjonale lovgivningen blir gjennomført.

Den Europeiske Menneskerettighetsdomstolen (EMD) har som hovedoppgave å sikre at forpliktelsene statene har påtatt seg etter EMK blir overholdt. Domstolens oppgave innebærer også at den tolker og utvider nedslagsområde for konvensjonen lovtekst.

---

[17] Augland, Mæland og Røsandhaug s. 107

Da artikkel 8 i EMK vil være den mest relevante bestemmelsen i konvensjonen sett i forhold til min problemstilling vil jeg kort redegjøre for bestemmelsen i det følgende.

2.7.2 EMK art. 8

Etter bestemmelsens første ledd har enhver borger krav på respekt for sitt privatliv, familieliv, sitt hjem og sin korrespondanse. Med korrespondanse mente konvensjonsteksten i utgangspunktet brev og postsendinger, men vil i dagens teknologiske samfunn også omfatte korrespondanse over telefon, telefax, mobiltelefoni, internett, e-post osv.[18]

At art. 8 første ledd også omfatter utlevering av trafikkdata ble slått fast av EMD i saken Malone vs. UK (1984). Malone var tiltalt for heleri og politiet hadde bygget mye av etterforskingen på trafikkdata mellom Malone og flere kjente kriminelle. Malone hevdet at myndighetene ikke hadde hjemmel i lov til å hente ut slike data. UK hevdet at innhenting av trafikkdata ikke var omfattet av art. 8. UK fikk ikke medhold i sine anførsler og EMD uttaler forholdsvis kontant at *"release of that information to the police without consent of the subscriber also amounts to the opinion of the Court to an interference with guaranteed by article 8."*

At bestemmelsen også kan anvendes på forhold hvor myndighetene overvåker personers bevegelser på internett, samt hvem personen ringer kommer klart frem av Copland vs. UK (2007). Copland var ansatt ved et universitet i England hvor arbeidsgiveren overvåket hvilke internettsider hun besøkte, hvilke telefonnummer hun ringte til og hvem som mottok e-post fra henne og hvem hun mottok e-post fra. Overvåkingen ble ansett for å være et brudd på retten til "private life" etter artikkel 8 når Copland verken hadde samtykket eller visste om slik overvåking. Myndighetene måtte her sørge for å utarbeide et lovverk som gikk klart av kravene som stilles opp i artikkel 8 annet ledd.

[18] Høstmælingen s. 229

At artikkel 8 også inneholder et visst vern mot at myndighetene foretar registrering av personopplysninger er slått fast i bl.a. Leander vs. Sweden (1987).

Etter artikkel 8 annet ledd kan myndighetene foreta inngrep som går utover de grunnleggende rettighetene som oppstilles i første ledd om dette er nødvendig for: *"national security, public safety, the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others."* I tillegg er det oppstilt et krav om at inngrepet er *"in accordance with the law"* og *"necessary in a democratic society"*.

"In accordance with law" innebærer at inngrepet må ha basis i norsk rett, samt at reglene må være tilgjengelige og forutsigbare. Om kontroll av kommunikasjon og innhenting av slik informasjon fra politiets side har EMD uttalt om dette kravet at: *"such measures must be based on a law that is particualry precise."*[19] Bakgrunnen for et slikt krav er at politimetodene blir mer og mer sofistikerte og personene som informasjonen omfatter ofte ikke kan kontrollere eller uttale seg det som eventuelt blir brukt under etterforskingen. Forutberegnlighet i lovverket er derfor en forutsetning for slike metoder. Begrepet "law" innebærer ikke bare skreven lov, men også uskreven lov og forskrifter.[20]

At tiltaket må være "necessary in a democratic society" innebærer at det foreligger et "pressing social need" for at inngripen etter annet ledd skal være tillatt.[21] I dette ligger det også et krav om proporsjonalitet mellom tiltaket og formålet myndighetene ønsker å oppnå.

Ordlyden i bestemmelsens annet ledd gir myndighetene en forholdsvis vid adgang til å gå bort fra rettighetene som oppstilles i første ledd. Men som vi har sett bl.a. gjennom Rt. 2009 s. 394 er bestemmelsen et viktig moment ved tolkningen av lovverket.

---

[19] Kruslin vs. France (1990) avsnitt 33

[20] Sunday Times vs. UK (1979)

[21] Sunday Times vs. UK (1979)

3 IDENTIFIKASJONSDATA

3.1 Innledning

Identifikasjonsdata skal i avhandlingen forstås som informasjon som direkte eller indirekte identifiserer en fysisk eller juridisk person. Direkte identifikasjon vil være opplysninger som navn eller fødselsnummer (eventuelt organisasjonsnummer). Indirekte identifikasjon vil være adresser, telefonnummer, IP-adresser og lignende.

Ekoml. har ingen definisjon av begrepet identifikasjonsdata, men en naturlig tolkning av ekoml. og ekomforskriften av 16. februar 2004 nr 401 tilsier at dette omfatter opplysninger om "sluttbrukeren" etter ekoml. § 1-5 nr 13. Sluttbruker er den som har inngått "avtale om tilgang til et elektronisk kommunikasjonsnett eller –tjeneste." Da det er denne personen tilbyderne har registrert i sine databaser, vil det være naturlig at det er identifikasjonsdata om sluttbruker som her omfattes.

For å kunne inngå en tilgangsavtale med en tilbyder er det normalt å oppgi fødselsnummer, org.nummer, etternavn, firmanavn, fornavn, mellomnavn, gatenavn eller postadresse, husnummer, postnummer, poststed og telefonnummer.[22] Dette er informasjon som tjenestetilbyderen i første omgang registrer på sine abonnenter[23] og må følgelig omfattes av begrepet identifikasjonsdata.

Etter ekoml. § 2-9 tredje ledd kan tilbyder uten hinder av taushetsplikten i første ledd gi opplysninger til politi og påtalemyndighet om "avtalebasert hemmelig telefonnummer eller andre abonnentopplysninger, samt elektronisk kommunikasjonsadresse."

Jeg vil i den første delen av dette kapittelet se på hvordan lovverket vedrørende identifikasjonsdata, og til dels også trafikkdata har utviklet seg ut fra et historisk

---

[22] Se vedlegg 1 og 2.

[23] Mer om begrepet under punkt 3.3.3

perspektiv. Hovedfokuset vil være på taushetspliktbestemmelsene som tilbyder og politiet har måttet forholde seg til.

3.2 Historisk tilbakeblikk

3.2.1 Telegrafloven (1899)

Da Lov om Eneret for Staten til Befordring af Meddelelser ved Hjælp av Telegraflinjer og Anlæg av 29. april 1899, heretter Telegrafloven, ble en del av det norske lovverket ga den etter § 1 første ledd i stor grad staten enerett til å: *"anlegge eller drive stasjoner eller innretninger til avsendelse eller mottagelse av meddelelser, toner, tegn, billeder og lignende ad elektrisk vei."*

Hvordan og til hvilken grad informasjonen som kom inn på disse anleggende ble lagret, tatt i mot og behandlet av ansatte eller i anlegget i seg selv ble ikke nevnt med et ord i loven, men gitt ved instruks. Hvordan instruksen og de enkelte bestemmelsene ble tolket var i stor grad opp til Televerket, og det forelå lite, til ingen offentlig informasjon vedrørende denne instruksen eller hvordan instruksen ble praktisert. Det kommer frem av Ot.prp.nr. 2 (1985-1986) s. 15 at instruksen bl.a. innebar at alle ansatte måtte avgi et løfte om å *"hemmeligholde for uvedkommende både hvem som har utvekslet telekorrespondanse og innholdet i korrespondansen."*

Når det gjelder utlevering av identifikasjonsdata kommer det frem av straffelovskommisjonens uttalelser i 1969 at abonnentdata nærmest rutinemessig ble utlevert til politiet ved anmodning og når det var igangsatt etterforsking. Kommisjonen gir eksemplet med telefonsjikane og at abonnenten ved slike tilfeller må anmode politiet om at identiteten til den mistenkte blir etterforsket.[24]

Da forvaltningsloven ved endringslov av 27. mai. 1977 nr. 40 ble gitt nye bestemmelser

[24] Innstilling om Rettergangsmåten i straffesaker av 1969 s. 257

vedrørende taushetsplikt var det planer om å gjennomgå særlovgivningen med tanke på å få tilpasset regelverket. Dette ble utsatt til samme året straffeprosessloven gjennomgikk sin lovendring av 1. januar 1986. Gjennomgangen viste at flere lovbestemmelser i særlovgivningen ble ansett for å være overflødige, mens andre særlover ble ansett for å være mangelfulle og gitt egne taushetspliktbestemmelser.

Telegrafloven ble ansett for å tilhøre sistnevnte gruppe og fikk ved lovendring av 16. mai 1986 nr. 21 en ny § 5 første ledd med følgende ordlyd:

> *"Alle som utfører tjeneste eller arbeid for Televerket plikter å bevare taushet overfor uvedkommende om det de i forbindelse med tjenesten eller arbeidet får vite om andres bruk av Televerket og om innholdet i telekorespondansen. De plikter også å påse at uvedkommende ikke får anledning til selv å skaffe seg kjennskap til slike opplysninger. Heller ikke kan de utnytte opplysninger som nevnt i denne paragraf i egen virksomhet eller i tjeneste eller arbeid for andre."*

Bakgrunnen for å ta bestemmelsen inn i Telegrafloven var fordi det i endringen som forelå i straffeprosessloven (1986) § 118 var satt opp at forbudet mot vitneforklaringer fra offentlige tjenestemenn uten samtykke fra departementet skal være begrenset til tilfelle hvor det foreligger lovbestemt taushetsplikt. Da taushetsplikten etter Telegrafloven var instruksbasert ville dette sammenfalle dårlig med arbeidet Televerket utførte og dermed deres forhold til kundene. I høringsnotatet til Ot.prp.nr. 2 (1985-1986) s. 15 uttaler Televerket at endringene i taushetsplikten *"i høy grad vil skade tillitsforholdet mellom Televerket og dets kunder"* og at man da *"ikke kan akseptere at den taushetsplikt som arbeidstakerne i Televerket i dag har overfor telekorrespondanse i fremtiden skal stå tilbake for den alminnelige vitneplikten"*

Uttalelsen tyder på at Televerket verdsetter taushetsplikten meget høyt og at den er viktig som begrensning i informasjonen som kommer ut av bedriften. Dette underbygges ved at Televerket senere i forarbeidet sammenligner sin egen taushetsplikt med den til dels

strenge taushetsplikten som forelå for postansatte i postlovens § 8.[25] Denne sammenligningen viser også at Televerket på denne tiden mottok informasjon som var sterkt innenfor den enkeltes personlige sfære. Televerket uttaler om dette:

> *"Slik korrespondanse står Televerket bare som formidler eller befordrer av mellom avsender og adressat. Innholdet i korrespondansen er i prinsippet Televerket helt uvedkommende."*[26]

Televerket understreker her at de kun fungerer som et nødvendig mellomledd mellom avsender og adressat. Innholdet av denne kommunikasjonen har Televerket tilgang til, men er bare et biprodukt av virksomheten og er Televerket "helt uvedkommende."

Hvem som ellers ble ansett å være "uvedkommende" etter § 5 i Telegrafloven blir ikke nærmere forklart i forarbeidene til loven, med unntak av presiseringen om at sjømilitære myndigheter ikke skal anses som uvedkommende. En kan tolke forarbeidene dit hen at for å ikke anses som uvedkommende måtte man være offentlig myndighet med legitim interesse i informasjonen. I tillegg må bakgrunnen for at informasjonen søkes være at det dreier seg om overtredelse av sentrale stats- og folkerettslige regler.[27]

Hvem som var berettiget til å få abonnentinformasjon ble ved lovendringen også meget uklart. Dette kommer blant annet frem av Ligningsmyndighetenes brev til Justisdepartementet av 20. mars 1991. Ligningsmyndighetene hadde her fått avslag på sin anmodning til Televerket om utlevering av navnet til en person som skjulte seg bak et hemmelig telefonnummer og ba derfor om en prinsipputtalelse vedrørende hvordan lovverket skulle tolkes. Lovavdelingen konkluderer med at slike abonnentopplysninger faller inn under "andres bruk av Televerket" og at dette er informasjon som faller inn under

---

[25] Ot.prp.nr. 2 (1985-1986) s. 15

[26] Ibid. s. 51

[27] Ibid. s. 52

taushetsplikten. Dette, uttaler departementet, er en naturlig tolkning i kravene som kommer frem av privatlivets fred.

Loven ble endret gjentatte ganger i løpet av 90-tallet, da hovedsakelig på grunn av avskaffelsen av Televerkets monopol[28] og senere ved endringen av Televerket til et AS.[29] Ved sistnevnte lovendring er det opplyst at det skjedde en endring i utleveringspolitikken til Televerket. Dette kommer blant annet frem av NOU 1997:15 hvor utvalget opplyser at identifikasjonsdata før disse lovendringene nærmest rutinemessig ble oppgitt til politiet ved etterspørsel ut fra prinsippene i forvaltningsloven § 13b nr. 5 og nr. 6.[30] Som vi skal se nedenfor gjorde endringen i denne utleveringspolitikken hverdagen betydelig vanskeligere for politiet.

3.2.2 Teleloven (1995)

Da Lov om telekommunikasjon av 23. juni 1995 nr. 39, heretter Teleloven, avløste Telegrafloven var det på høy tid. Dette blir særlig understreket innledningsvis i Ot.prp. nr. 36 (1994-1995) hvor det blir påpekt at gjeldende lovgivning er fra slutten av forrige århundre og at det *"er det nødvendig å erstatte denne lovgivningen med en lovgivning som på en bedre måte enn det eksisterende lovverk vil kunne gjenspeile den faktiske og rettslige situasjon."*[31]

Selv om innledningsordene i forarbeidet til den nye loven gir et håp om klarhet og forutberegnlighet i lovverket sto en av de mest uklare lovbestemmelsene fra den gamle loven, § 5, fortsatt uforandret. Dette hadde lovgiver forsøkt avhjulpet ved å gi forarbeider som definerte ordbruken i bestemmelsen bedre . "Andres bruk" ble for første gang definert og gitt betydningen:

---

[28] Lovendring av 4. juni 1993 nr. 60

[29] Lovendring av 24. juni 1994 nr. 45

[30] NOU 1997:15

[31] Ot.prp.nr. 36 (1994-1995) s. 3

> *"egne ansatte og kunders og andre og andre forretningsforbindelser, samt alle andre personers, bedrifters eller myndigheters bruk av telekommunikasjon."*[32]

Forarbeidet understreker i tillegg at *"taushetsplikten innebærer også plikt til å aktivt hindre at uvedkommende får tilgang til opplysningene."*[33]

Fortsatt var ikke Teleloven utstyrt med en egen utleveringsbestemmelse om abonnentinformasjon til politiet slik som nåtidens ekomlov § 2-9 tredje ledd. Hvem som var uvedkommende etter lovens ordlyd var derfor fortsatt uklart.

Spørsmålet om politiet måtte gå rettens vei ved å få utlevert identifikasjonsdata om hvem som var bak et hemmelig telefonnummer ble understreket igjen av Justisdepartementets lovavdeling i brev av 22. november 1995. Lovavdelingen konkluderer her med at både lovens ordlyd og reelle hensyn taler for en slik streng tolkning.

Problemene dette lovverket skapte for politiet i en etterforskingssituasjon var åpenbare. Ved enkle anmodninger om identifikasjonsdata om hvem som skjulte seg bak et hemmelig telefonnummer måtte politiet gå den "tunge" veien gjennom Statens Teleforvaltning, jfr. strpl. § 118 første ledd.

Problemet i lovverket ble belyst av utvalget i NOU 1997:15 som går så langt som å si at:

> *"Etterforskningen kan bli skadelidende, og i enkelte tilfeller forspille, ved å avvente avgjørelsene fra teleforvaltningen og retten."*[34]

---

[32] Ot.prp.nr. 36 (1994-1995) s. 44

[33] Ibid. s. 44

[34] Punkt 6.3

Utvalget fant denne metoden som unødvendig tidskrevende i en politihverdag som ofte krevde raske avklaringer og effektive etterforskningsmetoder og foreslo at bestemmelsen skulle endres slik at politiet skulle få raskere tilgang til identifikasjonsdata vedrørende hemmelige telefonnummer.

Forslaget ble vedtatt (med en utvidelse i tredje ledd) og ga følgende endring i Teleloven ved lovendring av 26. juni 1998 nr 53:

> *"Taushetsplikten er ikke til hinder for at det gis opplysninger til påtalemyndigheten eller politiet om en abonnents navn, adresse, telefonnummer eller datakommunikasjonsadresse. Det samme gjelder vitnemål for retten."*

Departementet uttaler vedrørende endringene at det *"ikke kan se at det er reelle hensyn som tilsier at opplysninger om en abonnents telefonnummer mv ikke skal kunne gis til politiet eller retten fordi vedkommende avtalemessig har fått tjenesteleverandøren til å gi seg et såkalt "hemmelig nummer""*[35]

Dette synspunktet blir nå hovedsakelig begrunnet i at abonnenten ikke har beskyttelsesverdig interesse i å skjerme disse opplysningene fra politiet. Utvidelsen i politiets adgang er i sterk kontrast til departementets egne uttaleser i brev av 1991 og 1995 hvor nektelse av slik utlevering nettopp begrunnes i reelle hensyn og retten til privatlivets fred.

Endringene i dette synet på hva som er underlagt taushetsplikt og hva som skal ha beskyttelsesverdig interesse må nok til dels søkes i den teknologiske utviklingen på midten av 90-tallet hvor flere fikk mobiltelefoner og datamaskiner. Dette førte til at politiets anmodninger steg betraktelig. I takt med utbredelsen av teknologien steg også antall kriminelle som ikke bare gjemte seg bak slike numre, men som også utførte kriminelle handlinger gjennom disse tjenestene. Lovgiver hadde nok tidligere ikke sett betydningen av

[35] Ot.prp.nr. 31 (1997-1998) s. 7

denne informasjonen for politiet og så nok heller ikke problemene som kunne oppstå på sikt med tanke på den teknologiske utviklingen.

3.3 Ekomloven

3.3.1 Innledning

Hovedregelen etter ekoml. § 2-9 første ledd at ”tilbyder og installatør” har taushetsplikt om ”innholdet av elektronisk kommunikasjon, og andres bruk av elektronisk kommunikasjon.”

Av § 2-9 tredje ledd fremgår det at de taushetsbelagte opplysningene etter første ledd ikke er til hinder for at det gis opplysninger til politi eller påtalemyndigheten om ”avtalebasert hemmelig telefonnummer eller andre abonnentopplysninger, samt elektronisk kommunikasjonsadresse.” Tredje ledds siste punktum klargjør at den samme informasjonen kan gis ved vitnemål for retten og at opplysninger etter § 2-9 første ledd også kan gis til annen myndighet i medhold av lov.

Jeg vil i det følende belyse hvilken type informasjon politiet kan få utlevert etter § 2-9 tredje ledd, samt belyse problemområdene som foreligger ved dagens lovverk.

3.3.2 Opplysninger om ”avtalebasert hemmelig telefonnummer”

Opplysninger om avtalebasert hemmelig telefonnummer vil si at tjenestetilbyderen må oppgi identifikasjonsdata om abonnenten som har avtale om hemmelig telefonnummer.

Det kommer frem av Ot.prp.nr. 58 (2002-2003) s. 93 at opplysninger om bruker av abonnement eller en telefon også vil omfattes av tredje ledd. Forarbeidene viser her til opplysninger som kan ”sammenlignes med opplysninger om hemmelig telefonnummer” og som derfor også er unntatt taushetsplikt. Forarbeidet gir eksemplene:

- *Hvilke SIM-kort som er knyttet til hvilket IMEI nr.*
- *Hvilke SIM-kort som er benyttet med samme IMEI nr.*
- *Hvilket telefonnummer som tilhører et SIM-kortnummer.*
- *Hvilket SIM-kort, og dermed telefonnummer som kan knyttes til en oppladning, uavhengig av lademetoden.*
- *IMSI nummeret til et SIM-kort.*

I tillegg til identifikasjonsdata om en abonnent som har tegnet et hemmelig telefonnummer forutsetter altså lovgiver at politiet her kan få utlevert opplysninger om SIM-, IMEI- og IMSI-nummer.

SIM (Subskriber Ideentity Module) er et smartkort som er nødvendig for at mobiltelefonen skal kunne koble seg opp mot riktig tilbyder og gi nødvendig nettverk. Kortet inneholder et unikt nummer (IMSI) som identifiserer brukeren i mobilsystemet slik at brukeren kan ringe og bruke telefonen som forutsatt.

IMEI (International Mobile Equipment Identity) er et nummer som består av 15 tall som identifiserer selve håndsettet.

IMSI (International Mobile Subscriber Identity) er nummeret som identifiserer et mobilabonnement i GSM-systemet. Dette nummeret lagres elektronisk i SIM-kortet og identifiserer teleoperatøren, uavhengig av hvilket land teleoperatøren kommer fra som har utstedt kortet.

I en etterforskingssituasjon er disse numrene av særlig viktighet ved at politiet kan samordne IMEI- og SIM-numre, og på den måten få god oversikt over mobiltelefoner og telefonnumre som kan knyttes til enkeltpersoner. I tillegg kan disse numrene hjelpe politiet med å identifisere håndsett som de mistenker er stjålet.

At ordlyden i bestemmelsen ikke kan sies å legge opp til slik utvidet tolkning som forarbeidene her legger til grunn er kritisert bl.a. av Leif-Henrik Rønnevig i sin kommentarutgave til ekomloven. Han legger da vekt på hensynet til klarhet og forutberegnlighet i lovverket og han understreker at mulighetene politiet her har burde "gått klarere frem av lovteksten." [36]

Forarbeidene legger til grunn at disse numrene *"kan sammenlignes med hemmelig telefonnummer"* og derfor i en viss grad kan leses ut av ordlyden i § 2-9 tredje ledd. Likheten mellom de to nummertypene er ikke umiddelbart påfallende, og forarbeidene gir ingen nærmere redegjørelse for hvordan disse numrene kan anses å være sammenlignbare med et hemmelig telefonnummer. En naturlig vinkling vil da være å se på hvilken type informasjon politiet får ved at disse numrene utleveres og den beskyttelsesverdige interesse en abonnent har for å holde slike numre hemmelige for politiet.

Lovgiver anser informasjonen som kommer frem ved utlevering av disse numrene for å være så lite inngripende overfor den et slikt pålegg retter seg mot at bestemmelsens ordlyd tolkes utvidende. Man har derfor nøyd seg med å nevne denne muligheten i forarbeidene. Legalitetsprinsippet forutsetter at bestemmelser som lovfester en adgang for myndighetene til å foreta inngrep i borgernes rettsfære skal være klare og tydelige, samt at man skal være forsiktige med å tolke ordlyden i slike bestemmelser utvidende.

Det faktum at slike nummer i all hovedsak kun omhandler enkeltpersoner taler i stor grad for en slik adgang som stilles opp i forarbeidet. I tillegg vil informasjonen som politiet her får utlevert være av stor betydning for etterforskingen, da håndsettene som brukes av for eksempel flere kriminelle kan identifiseres lettere. I tillegg vil den raske utviklingen som skjer på området tale for en videre adgang til å fortolke slike muligheter inn i lovverket – dersom lovverket stengte for slike tolkninger ville man være tvunget til å oppdatere bestemmelser som gir slike muligheter meget ofte. I tillegg – og noe igjen som taler for en

[36] http://abo.rettsdata.no/browse.aspx?sDest=gL20030704z2D83

slik adgang - vil være det faktum at informasjonen som utleveres er av meget upersonlig og lite inngripende karakter. Numrene er fastlåst i telefonen eller i kortet og vil ikke gi annen informasjon enn selve nummeret som søkes, eventuelt annen identifikasjonsdata som er unntatt fra taushetsplikten etter § 2-9 tredje ledd.

I tillegg er forarbeidene klare på at listen med SIM, IMEI og IMSI- nummer ikke er uttømmende, jfr. bruken av ”for eksempel” og ”kan sammenlignes med”. Det kan derfor tenkes at bestemmelsen også hjemler andre utleveringsforpliktelser for tilbyderne så lenge informasjonen kun gir opplysninger om ”bruker av et abonnement eller en telefon.”

Det må nevnes at sammenhengen i lovverket taler i mot en slik utvidende tolkningen av tredje ledd. Det følger av ekoml. § 12-4 nr. 2 at overtredelse av taushetsplikten i § 2-9 første ledd kan straffes med bøter eller fengsel i inntil seks måneder. Dersom det åpnes for utvidende tolkninger av slike bestemmelser vil man her undergrave taushetsplikten som lovgiver har forutsatt og straffesanksjonert. Slike tolkningsmuligheter kan også gi uklare perimetre for hva som skal falle inn under §2-9 tredje ledd ved at tolkningsmulighetene er såpass vide. Dette igjen kan gi et uklart lovverk hvor tilbyderne kan tenkes å tolke bestemmelser forskjellig, og på den måten vanskeliggjøre politiets arbeid ved at det sjelden foreligger faste rutiner på området. At tilbyderne tolker lovverket forskjellig har gitt politiet betydelige problemer ved utlevering av slike data tidligere (se punkt 4.4.2).

En avveining mellom de ovennevnte momentene taler for en mulighet for å kunne tolke § 2-9 tredje ledd utvidende. Legalitetsprinsippet og lovkravene som stilles opp i EMK art. 8 vil ikke komme inn med full styrke, da utleveringen av slike opplysninger ikke kan sies å være innenfor den personlige sfære. I tillegg vil informasjonen som politiet får utlevert være til stor hjelp under etterforskingen. Adgang til en utvidende tolkning av § 2-9 tredje ledd støttes også av førstvoterendes premisser i kjennelsen inntatt i Rt. 1999 s. 1944 (se punkt 3.3.4).

Et spørsmål som etter dette må stilles er om utlevering av PUK-koder omfattes av § 2-9 tredje ledd. Dette er passordkoder som beskytter SIM-kortet slik at uvedkommende ikke får adgang til innholdet i kortet eller får koblet håndsettet opp mot et telenettverk (med unntak av nødnummer i de fleste land). Samferdselsdepartementet har i brev til PT av 27.3.2009 konkludert med at PUK-koder faller inn under taushetsbelagte opplysninger i ekoml. § 2-9 første ledd. I samme brev kommer det også frem at en endring i denne praksisen krever lovendring. Samferdselsdepartementets tolkning må her kommenteres.

Etter § 2-9 første ledd skal det bevares taushet om ”innholdet av elektronisk kommunikasjon” og ”andres bruk av elektronisk kommunikasjon, herunder opplysninger om tekniske innretningen og fremgangsmåter”. Utlevering av PUK-koder kan vanskelig sies å falle inn under ordlyden til det som etter § 2-9 regnes for å være taushetsbelagt informasjon.

For det andre er det klart at taushetspliktbestemmelsene historisk sett er opprettet for at abonnenten skal *”formidle korrespondanse over telenettet uten frykt for at korrespondansen kommer til uvedkommendes kjennskap.”*[37] Trafikkdata er informasjon som lagres hos en tilbyder, og som sluttbrukeren – når han har foretatt en handling på mobiltelefonen eller over internett - ikke har kontroll over. Noen likhetstrekk med ”korrespondanse” har PUK-koder ikke.

Det er klart at PUK-koder heller ikke faller inn under noen av unntakene i § 2-9 tredje ledd. PUK-koder kan dermed verken anses som trafikkdata eller identifikasjonsdata. Slike koder faller derfor mellom to stoler i det gjeldende lovverket.

Det må understrekes at SIM-kortet kan lagre en del informasjon som bærer preg av å være taushetsbelagt. Både innholdet av tekstmeldinger, A- og B-nummer, hvor lenge samtalene har vart, samt bilder og annen informasjon kan lagres i kortet, og taler for en streng adgang

[37] Ot.prp.nr. 2 (1985-1986) s. 15

til disse kodene. Den beskyttelsesverdige interessen til disse kodene er derfor større enn den som foreligger ved for eksempel utlevering av IMSI nummer.

Etter dette er det klart at utlevering av PUK-koder har større beskyttelsesverdig interesse enn det som ”kan sammenlignes med hemmelig telefonnummer”, men at ordlyden i § 2-9 første ledd gir taushetsplikt for slik informasjon kan jeg ikke se. Samferdselsdepartementet har derfor tolket 2-9 første ledd utvidende til også å gjelde slike numre. Tolkningen er i henhold til legalitetsprinsippet som gir en vid adgang til å tolke loven til å gjelde utenfor sin ordlyd, når dette er til fordel for borgerne.

Hensynene til forutberegnlighet og klarhet i lovverket gjør at det hadde vært ønskelig med en klarere lovhjemmel, både for hva som omfattes av taushetsplikten etter § 2-9 første ledd, men også hva som omfattes av unntakene for taushetsplikt i § 2-9 tredje ledd.

3.3.3 ”Andre abonnentopplysninger”

Selv om ”abonnent” er nevnt flere ganger i ekoml., både i § 2-7 første ledd (”abonnenten”) og i § 2-9 tredje ledd (”abonnementsopplysninger”) – samt flere ganger i forarbeidene, er det ikke nærmere definert i loven. En naturlig forståelse av ordet, samt hvordan begrepet blir brukt i forarbeidene og i loven tilsier at ”abonnent” skal forstås som ”sluttbruker” etter § 1-5 nr. 13. En ”sluttbruker” er etter bestemmelsen den som har inngått ”avtale om tilgang til et elektronisk kommunikasjonsnett eller –tjeneste.” Da identifikasjonsdata/abonnentopplysningene kun kan omfatte opplysninger som er registrert på en avtalefestet bruker, og dermed direkte eller indirekte identifisere denne som en fysisk eller juridisk person, vil jeg legge denne forståelsen til grunn.

Under punkt 3.1 er det listet opp en del registreringsinformasjon som er nødvendig å oppgi for å kunne bli kunde hos en leverandør av en elektronisk kommunikasjonstjeneste. Den samme informasjonen plikter tilbyder av offentlig telefontjeneste etter ekomforsikriften § 6-3 å stille til tilbydere av opplysningstjeneste, når informasjonen skal nyttes i nummeropplysningstjeneste. En naturlig forståelse av lovverket, samt reelle hensyn taler i

stor grad for å gi politiet tilgang til denne informasjonen ved anmodning etter § 2-9 tredje ledd, sml. vurderingen i Ot.prp.nr. 31 (1998-1999) s. 8.

3.3.4 "Elektronisk kommunikasjonsadresse"

Etter Ot.prp.nr. 58 (2002-2003) s. 93 er det klart at "elektronisk kommunikasjonsadresse" omfatter "navn, adresse og telefonnummer tilknyttet en elektronisk kommunikasjonsadresse." Forarbeidet viser eksplisitt til kjennelsen inntatt i Rt. 1999 s. 1944 og at begrepet skal tolkes i lys av kjennelsen. Selv om kjennelsen omhandler begrepet "datakommunikasjonsadresse" i Teleloven (1995) § 9-3 tredje ledd, er innholdet i de to begrepene det samme, jfr. "bestemmelsen er en videreføring av bestemmelsene i teleloven om taushetsplikt."[38]

I kjennelsen var det uenighet mellom Økokrim og tjenestetilbyderen Nextel om rekkevidden av teleloven § 9-3 tredje ledd og hvor langt begrepet "datakommunikasjonsadresse" skulle forstås. Økokrim hevdet at de kunne kreve å få oppgitt navnet på en abonnent som var koblet til internett med et vertsnavn på et bestemt tidspunkt og som hadde formidlet barnepornografisk materiale. Politiet begjærte i tillegg utlevert det telefonnummer som ble benyttet ved tilkoblingen. Begjæringen ble sendt til Post- og Teletilsynet som tolket informasjonen Økokrim ville ha utlevert til å omfattes av unntaket for taushetsplikt i § 9-3 tredje ledd.

Nextel på sin side hevdet at bestemmelsen ikke ga rammer for slik utlevering, bl.a. med grunnlag i at bestemmelsen kun omfatter statiske datakommunikasjonsadresser. I denne saken var brukeren pålogget med en dynamisk IP-adresse, d.v.s. en identifikasjonsadresse som endres for hver pålogging. Nextel var derfor av den oppfatning at *"politiet må gå frem på den måten som er angitt i straffeprosessloven § 118."*[39]

---

[38] Ot.prp.nr. 58 (2002-2003) s. 93

[39] Rt. 1999 s. 1944, s. 1946

Når det gjaldt utlevering av informasjon om en abonnents datakommunikasjonsadresse uttaler førstvoterende at bestemmelsen ikke kan tas på ordet, men at den skal tolkes innskrenkende.[40] Videre legger han vekt på personvernet og at:

> *"det må stilles krav til innholdet av politiets spørsmål."*[41]

Spørsmålet som deretter måtte løses var om innholdet i politiets spørsmål var godt nok når:

> *"politiet spør om abonnentens navn på grunnlag av én vertsadresse og ett bestemt klokkeslett som – det er enighet om – entydig utpeker abonnenten."*[42]

Ovennevnte spørsmål fra politiet ble ansett for å være konkret nok av førstvoterende. Det ble videre diskutert om en IP-adresse med tidspunkt for oppkobling er en datakommunikasjonsadresse. Dette vil ikke førstvoterende ta endelig stilling til, men han:

> *"antar at det kan være naturlig ut fra antydninger i forarbeider å se denne kombinasjonen av en dynamisk IP-adresse og tidspunktet da adressen ble benyttet, for å falle inn under uttrykket, og dette kan sies å styrke den lovtolkning jeg anser for den rette."*[43]

Førstvoterende går så inn på en drøftelse om lagmannsretten har tolket loven riktig når Nextel er pålagt å opplyse om navnet på abonnenten så vel som det nummer det ble ringt fra. Førstvotende legger først til grunn at lagmannsretten har tolket loven riktig, selv om ordlyden i § 9-3 tredje ledd trekker i retning at det kun er abonnentens eget telefonnummer som kan oppgis. Førstvoterende forklarer dette ved at bestemmelsen må:

---

[40] Ibid. s. 1949

[41] Ibid.

[42] Ibid. s. 1950

[43] Ibid. s. 1951

> *" forstås slik at operatøren kan oppgi ikke bare abonnentens nummer, men også det telefonnummer som ble benyttet ved koblingen til internett. Denne tolkningen tilsies av sammenhengen mellom opplysningene."*[44]

Det foreligger altså et prinsipp om sammenheng mellom opplysninger, og vil si at når opplysninger peker mot en annen, *"skal også den andre utleveres såfremt den etter sin art er omfattet av bestemmelsen."*[45] Dette synspunktet blir også fulgt opp i Rt. 2000 s. 169.[46]

Sammenhengen i lovverket blir også tillagt vekt når førstvoterende sammenligner hemmelig identitet som følge av tekniske forhold med hemmelig identitet som følge av avtale. Etter å ha sett på formålet med lovendringen i Ot.prp.nr. 31 (1997-1998) konkluderer han med at:

> *"det er grunn til å peke på at opplysning om abonnentens navn på grunnlag av et IP-nummer som er tildelt for bruk på et bestemt tidspunkt, har atskillig likhet med en opplysning om hvem et bestemt hemmelig telefonnummer tilhører, selv om anonymiteten i siste tilfelle er knyttet til avtale, mens den her beror på tekniske begrensninger i systemet. I begge tilfeller dreier det seg om abonnentopplysninger. Etter min mening er det liten grunn til å behandle tilfellene forskjellig slik at politiet i vårt tilfelle skal måtte bruke den mer omstendige fremgangsmåten etter straffeprosessloven § 118."*

Forholdet til EMK art. 8 blir også belyst av førstvoterende som kommer til at hans syn ikke strider mot bestemmelsen. Mye tyder på at førstvoterende her er enig i politiets anførsler på side 1948 hvor det anføres at:

> *"sterke reelle hensyn tilsier at politiet får slike opplysninger hurtig for å kunne bekjempe den stadig tiltakende kriminalitet som foregår via internett."*

---

[44] Ibid. s. 1952

[45] Sunde s. 283

[46] Se Rt. 2000 s. 169, s. 172

Førstvoterende konkluderer så med at lagmannsretten har lagt til grunn korrekt tolkning av loven og at *"så vel navnet på abonnenten som det nummer som ble ringt fra er nødvendige for at politiet skal kunne oppspore den person det gjelder, og at nummeret derfor kan oppgis."*[47]

Kjennelsen klargjorde flere elementer i et uklart lovverk. For det første ble det klart at det foreligger en utleveringsplikt for tilbyder når politiet opplyser om vertsadressen og det klokkeslett vertsadressen ble benyttet, med andre ord hvor opplysningene som søkes utlevert er tilstrekklig konkretisert og entydige. Identifikasjonsopplysningene man da fikk utlevert ga igjen hjemmel for å få utlevert ytterligere opplysninger, da om hvilket telefonnummer som ble benyttet til å foreta oppkoblingen.

Kjennelsens premisser forutsetter også at det ved tolkningen av regelverket skal legges vekt på sammenhengen i lovverket, formålet med bestemmelsene, krav til entydighet fra den som anmoder om utlevering og den teknologiske utviklingen som skjer på området. Dette er spesielt viktig når det gjelder et slikt rettsområde hvor det – som førstvoterende uttaler i kjennelsen *"skjer en raskt teknisk utvikling."*[48]

At kjennelsen var viktig illustreres godt ved at den blir nevnt eksplisitt i forarbeidene til ekomloven hvor den nærmest blir brukt som et ankerpunkt ved utarbeidelsen av § 2-9 tredje ledd. At avgjørelsen er viktig støttes også av etterfølgende rettspraksis på området, se bl.a. Rt. 2000 s. 169.

Det må nevnes at den dissenterende dommer i 1999-kjennelsen legger seg på en annen linje enn flertallet, og er av den oppfatning at fremgangsmåten i § 9-3 tredje ledd ikke er i godt nok samsvar med prinsippene i EMK artikkel 8, og at påtalemyndighetene derfor må gå frem etter reglene i strpl. § 210, jfr. § 118.

---

[47] Rt. 1999 s. 1944, s. 1952

[48] Ibid. s. 1950

3.4 Utleveringsplikt?

Ved anmodning fra politiet om utlevering av informasjon som nevnt i § 2-9 tredje ledd har tjenestetilbyderen plikt til at anmodningen etterkommes. Dette kan leses ut av § 2-9 fjerde ledd hvor det fremkommer at anmodningen ”skal etterkommes”. Unntak fra denne plikten kan kun forekomme om det foreligger ”særlige forhold” som gjør utleveringen ”utilrådelig.”

Unntaket ble tenkt som en sikkerhetsventil for tjenestetilbyderen i saker som ikke er satt under etterforskning. Forarbeidene nevner som eksempel: ”forvaltningssaker og namssaker.” [49] Unntaket kan også tenkes å komme til anvendelse på saker hvor det er mulighet for at opplysningene fører til forvekslingsfare[50], for eksempel der tjenestetilbyderen ser at det åpenbart er en feil i registreringsrutinene eller lignende.

3.5 Anmodningens innhold

Plikten til å utlevere informasjon til politiet etter § 2-9 tredje ledd krever ikke at politiet oppgir noen grunn for hvorfor de søker disse opplysningene, at det er utpekt en mistenkt eller siktet eller at det er igangsatt etterforsking.[51] Bakgrunnen for dette er at informasjonen som søkes utlevert også skal kunne hjelpe politiet i sine daglige og sivile gjøremål som for eksempel oppgaver for forvaltningen og namsmannen, samt at politiet i starten av en etterforskingsfase gjerne har lite informasjon om mistenkte, og informasjonen som da søkes utlevert gjerne vil hjelpe til å styrke eller svekke mistanker mot de involverte parter.[52]

Når det er sagt krever § 2-9 tredje ledd at man har informasjon som viser til en viss type identifikasjon, det være seg indirekte eller direkte. Dersom slik informasjon ikke foreligger

---

[49] Ot.prp.nr. 31 (1997-1998) s. 16

[50] Sunde s. 289

[51] Ot.prp.nr. 58 (2002-2003) s. 94

[52] Ot.prp.nr. 31 (1997-1998) s. 8

et det klart etter 1999-avgjørelsen et krav at opplysningene gir en entydig anvisning på identitet og sammenheng mellom opplysningene.[53]

3.6 Avsluttende bemerkninger

Etter dagens lovverk har politiet en vid mulighet til å sikre seg identifikasjonsdata om abonnenter på de grunnlag som stilles opp i § 2-9 tredje ledd. På grunn av den teknologiske utviklingen som skjer på området, samt det faktum at identifikasjonsdata ikke regnes for å være taushetsbelagt informasjon etter § 2-9 første ledd, er det åpnet for utvidende tolkning når det gjelder bruken av tredje ledd.

I tillegg har muligheter som den nye teknologien bringer med seg gjort at også taushetspliktbestemmelsen i § 2-9 første ledd også tolkes til å gjelde utenfor sin ordlyd. Jeg tenker da spesielt på PUK-koder som faller mellom ordlyden i både § 2-9 første ledd og tredje ledd. I slike tilfeller veier derfor personvernhensyn, informasjonens beskyttelsesverdige interesse og legalitetsprinsippet veie tyngre enn hensynet til en effektiv etterforsking.¨

[53] Sunde s. 289

4 TRAFIKKDATA

4.1 Innledning

Trafikkdata, vil som identifikasjonsdata, være informasjon som politiet anmoder om å få utlevert fra en tilbyder av en elektronisk kommunikasjonstjeneste. Dataene inneholder informasjonen som regnes for å være mer inngripende overfor den som berøres av utlevering enn identifikasjonsdata og er derfor underlagt taushetsplikt etter ekoml. § 2-9 første ledd.

Hva trafikkdata består av blir definert litt forskjellig avhengig av om man søker trafikkdata generert fra mobiltelefoner eller fra internettbruk. Når det gjelder mobiltelefoner blir innholdet av trafikkdata definert slik i Ot.prp.nr. 64 (1998-1999) s. 52:

> *"opplysninger om hvilke telefoner som i et bestemt tidsrom skal settes eller har vært satt i forbindelse med hverandre, om samtalens varighet og om teleabonnentens adresser. For mobiltelefoner kan det også opplyses om i hvilke geografiske områder oppringer og mottaker befinner seg."*

En mer internettsentrert beskrivelse kommer frem av Ot.prp.nr. 58 (2002-2003) s. 92 som gir trafikkdata følgende innhold:

> *"Med trafikkdata menes for eksempel data som angir kommunikasjonens opphavssted, bestemmelsessted, rute, klokkeslett, data, omfang, varighet og underliggende tjeneste."*

Trafikkdata blir i ekomforskriften § 7-1 første ledd definert som data som er *"nødvendig for å overføre kommunikasjon i et elektronisk kommunikasjonsnett eller for fakturering av slik overføring."*

Avhandlingen vil i det følgende gi en oversikt over hvordan trafikkdatabegrepet har forandret seg med tiden, og hvordan regelverket hva gjelder utlevering av disse dataene har

utviklet seg. Når det er sagt vil hovedfokuset i denne delen av avhandlingen problematisere lovverket som foreligger på rettsområdet i dag.

4.2 Historisk tilbakeblikk

Da lovverket som omhandler taushetsplikten for tilbyder vedrørende trafikkdata kommer frem av min redegjørelse under punkt 3.2 vil jeg fokusere på hva straffeprosessloven har lagt i begrepet og hvor beskyttelsesverdig denne informasjonen er blitt ansett. Historiske tilbakeblikk vil også gjøres fortløpende i teksten hvor dette faller naturlig.

Som vi har sett over har tilbyderne alltid vært underlagt en forholdsvis streng taushetsplikt hva gjelder hvem som skal få informasjon om slike data. Når det er sagt har straffeprosesslovens bestemmelser ikke alltid vært like gjennomtenkt og stilt like strenge krav til hvordan trafikkdata kan hentes ut og brukes av politiet.

Allerede ved lov om kontroll med post og telegrafforsendelser og telefonsamtaler av 24. juni 1915 ble det oppstilt en mulighet for myndighetene å føre kontroll med telegrafforsendelser og telefonsamtaler, herunder også det som i dag kalles for trafikkdata. Loven var en fullmaktslov og ga myndighetene muligheter til å utføre kontroll under krigstid med de fleste typer av forsendelser ”av hensyn til rikets sikkerhet.” Loven ble endret og utvidet flere ganger i årenes løp, bl.a. ble den ved lovendring av 15. desember 1950 nr. 5 ble gitt utvidet anvendelsesområde ved å sette opp materielle straffekrav for dens anvendelse. Ved lov av 3. desember 1999 ble loven opphevet da gjennom innføringen av strpl. § 212 og straffeprosesslovens kapittel 16a.[54]

Straffelovskomiteens uttaleser ved revisjonen av straffeprossloven i 1969 illustrer datidens syn vedrørende trafikkdata på en god måte. Komiteen utaler at de anser det for *”ubetenkelig med en forholdsvis vid hjemmel”* for annen telefonkontroll som ikke omfatter

[54] NOU 2004:6 s. 74

avlytting.[55] Ved bruk av trafikkdata så komiteen heller ingen andre begrensninger enn at dette kunne skje ved *"grunn til mistanke om en handling som etter loven medfører frihetsstraff."*

Synet på telefonkontroll som ikke er avlytting må sies å ha endret seg betraktelig siden 1969, og som vi skal se nedenfor er det nå flere hensyn som nå ligger bak regelverket som hjemler bruk av trafikkdata etter straffeprosessloven.

4.3 Lagring av trafikkdata

4.3.1 Innledning

Det kommer frem av ovennevnte definisjoner av begrepet "trafikkdata" at det foreligger to former trafikkdata. Jeg velger å kalle disse formene for kommunikasjonsdata og lokasjonsdata.[56] Begrepene er gitt forskjellige navn under andre forfattere[57], men innholdet i begrepene er de samme.

4.3.2 Kommunikasjonsdata

Kommunikasjonsdata forteller "tidspunkt for start og slutt av samtalen, hvilket nr. det blir ringt fra (A-nr) og hvilket nr. det blir ringt til (B-nr)."[58] Kommunikasjonsdata kan fortelle hvilken enhet som har vært del i kommunikasjonen og til hvilken tid enheten utførte kommunikasjonen. Med andre ord; data om selve hendelsen, og som er nødvendig informasjon for tilbyderen for at brukerne av en elektronisk kommunikasjonstjeneste skal komme i kontakt med hverandre og for korrekt fakturering.

---

[55] Innstilling om Rettergangsmåten i straffesaker s. 257

[56] Willassen (2010) s. 5, Norsk Regnesentral "Rapport om Elektroniske Spor" 2005 s. 27

[57] Se bl.a. Sunde s. 271 som bruker ordet "posisjonsdata"

[58] Norsk Regnesentral (2005) s. 27

4.3.3 Lokasjonsdata

Lokasjonsdata er informasjon om brukerens lokasjon ved kommunikasjonstidspunktet – eller rettere sagt: hvilken basestasjon brukeren benytter seg av ved kommunikasjonen. Denne informasjonen blir hovedsakelig lagret for faktureringsformål for å gi sluttbrukeren riktig takst i forhold til kontaktet basestasjon.

4.3.4 Historiske trafikkdata, fremtidige trafikkdata og trafikkdata i sanntid

4.3.4.1 Innledning

Trafikkdata kan igjen deles inn i tre tidsgrupper avhengig av hva politiet begjærer utlevert. Disse kalles for: historiske trafikkdata, fremtidige trafikkdata og trafikkdata i sanntid. Regelverket for hva som kan hentes ut er her forskjellig og vil bli behandlet mer inngående nedenfor i avhandlingen der dette faller naturlig. I det følgende kommer en kort gjennomgang av hva begrepene omfatter.

4.3.4.2 Historiske trafikkdata

Dette er trafikkdata som allerede er generert og lagret i en database hos en tjenestetilbyder. Dette regnes for å være den minst inngripende formen for trafikkdata å utlevere, da informasjonen allerede foreligger og er generert ved utleveringsbeslutningen.

4.3.4.3 Fremtidige trafikkdata

Fremtidige trafikkdata er data som politiet kan få utlevert så fort det genereres. Hjemmelen for slik utlevering er strengere enn for utlevering av historiske data.

4.3.4.4 Trafikkdata i sanntid

Trafikkdata i sanntid vil si at politiet selv genererer sporet ved å sende ut for eksempel en skjult tekstmelding til en mobiltelefon. Ved hjelp av informasjonen som kommer tilbake vil politiet for eksempel kunne oppspore personen ved hjelp av lokasjonsdata.

4.3.5 Kort om teletilbydernes lagringspraksis

Det foreligger ingen plikt for tilbyderne å lagre trafikkdata av hensyn til kriminalitetsbekjempelse. Tvert i mot er lovverket lagt opp slik at tilbyderne kun kan lagre trafikkdata med hensyn til fakturerings- eller kommunikasjonsformål, jfr. ekoml. § 2-7 annet ledd. Når disse opplysningene ikke lenger er nødvendige for disse formål må de anonymiseres eller slettes, jfr. § 2-7 annet ledd.

Trafikkdata fra mobiltelefoner lagres i alt fra 3 til 5 måneder etter at informasjonen blir registrert. Spennet i lagringen forklares i forskjellige betalingsfrister, kundens eget behov og utgangstiden på klageadgangen. Når det gjelder tilbydere av internett og lagring av trafikkdata er adgangen til å lagre slik informasjonen kun tre uker etter et vedtak fra Datatilsynet i 2009.[59] Vedtaket er en effekt av utviklingen i internettmarkedet hvor man i dag stort sett betaler en fastpris hver måned for ubegrenset internettilgang. Rapporter fra internettleverandørene tilsier at dette vedtaket i stor grad er blitt overholdt.[60]

Etter § 2-7 tredje ledd, siste punktum settes det opp et krav om samtykke dersom tilbyder skal utføre ”annen behandling av trafikkdata”. Her mener lovgiver *”enhver bruk av trafikkdata, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter”*.[61] Regelen klargjør forholdet til personopplyningsloven og kravene som oppstilles ved behandling av slik informasjon etter persl. § 2 nr. 2. Samtykket må derfor følge kravene som oppstilles i persl. § 2 nr. 7 – samtykket skal være en utrykkelig, frivillig og informert erklæring hvor det fremkommer at den registrerte godtar behandlingen av opplysningene.

---

[59] Willassen (2010) s. 16

[60] Ibid.

[61] Ibid.

4.3.6 Kort om tjenestetilbyderens tilretteleggingsplikt

Ekoml. § 2-8 første ledd pålegger tilbyder å tilrettelegge nett og tjeneste slik at lovbestemt tilgang til informasjon om "sluttbruker og elektronisk kommunikasjon sikres". Dette kravet blir i Ot.prp.nr. 58 (2002-2003) s. 93 regnet for å gjelde *"kommunikasjonskontroll som gjennomføres av politiet etter reglene i straffeprosessloven kapittel 16a"*. Det blir i forarbeidet understreket at kravet gjelder både for innholdet i kommunikasjonen og for trafikkdata, samt *"utleveringspålegg etter strpl. § 210 når utleveringspålegget gjelder informasjon om sluttbruker og elektronisk kommunikasjon."*[62]

Det understrekes at tilbyder etter bestemmelsen kun plikter å tilrettelegge for en slik tilgang. Bestemmelsen gir ingen lovbestemt plikt til å lagre informasjonen av disse grunner.

4.4 Politiets adgang til trafikkdata

4.4.1 Innledning

Hovedregelen etter ekoml. § 2-9 første ledd er som kjent at "tilbyder og installatør" har taushetsplikt om "innholdet av elektronisk kommunikasjon, og "andres bruk av elektronisk kommunikasjon."

For det første er det klart at tilbyderen har taushetsplikt om innholdet av elektronisk kommunikasjon. Dette kan for eksempel omfatte innholdet i en SMS, eller en e-post eller hva som blir sagt i en telekorrespondanse.

For det andre foreligger taushetsplikt om "andres bruk av elektronisk kommunikasjon". Det motsatte av "andres bruk" er egen bruk. Det er med bakgrunn i dette klart at taushetsplikten

[62] Ot.prp.nr. 58 (2002-2003) s. 93

ikke gjelder når parten i en kommunikasjon det søkes trafikkdata om har samtykket til utlevering.[63]

Etter § 2-9 fjerde ledd kan Samferdselsdepartementet (”myndigheten”), gi nærmere forskrifter om taushetsplikten, se bl.a. ekomforskriften § 7-1 første ledd hvor tilbyder skal ”bevare taushet om trafikkdata”.

Politiet kan velge flere fremgangsmåter for å få utlevert trafikkdata fra tilbyderne. Jeg vil i det følgende nevne disse metodene, og problematisere regelverket i henhold til min problemstilling.

4.4.2 Fritak fra Post- og Teletilsynet

Hovedregelen etter strpl. § 108 er at ”enhver plikter” å ”forklare seg overfor retten, med mindre annet er bestemt ved lov”. Det kommer frem av § 118 første ledd at retten ikke kan ta i mot forklaring fra ”tilbyder av tilgang til elektronisk kommunikasjonsnett eller elektronisk kommunikasjonstjeneste…” som krenker lovbestemt taushetsplikt med mindre det foreligger ”samtykke fra departementet.” Adgangen til å gi slikt samtykke ligger i utgangspunktet hos Samferdselsdepartementet, men denne adgangen er delegert til Post- og Teletilsynet (PT) ved delegasjonsvedtak av 15. september 1995 nr. 39.

PT kan nekte tilbyderen fritak fra taushetsplikten om åpenbaringen vil kunne utsette staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighold, jfr. § 118 første ledd, tredje punktum.

PT opplyser at det med bakgrunn i ovennevnte bestemmelse gjøres en konkret rimelighetsvurdering etter de samme vurderingsmomentene som oppstilles i strpl. § 170a. Det legges vekt på personens straffeprosessuelle stilling som siktet eller mistenkt, om det foreligger skjellig grunn til mistanke om det er utført en straffbar handling, hvor viktig er

[63] Mer om samtykke under punkt 4.3.5

dataene for politiet i etterforskningssituasjonen og om politiet kan benytte seg av mindre inngripende metoder for å nå sitt mål. For utlevering av lokasjonsdata opplyser PT at det i vurderingen også legges vekt på befolkningstettheten rundt basestasjonen, det straffbare forholdets alvorlighet og på hvilken tid av døgnet begjæringen strekker seg fra.[64]

Dersom vitneplikten oppheves, og tilbyder kan forklare seg til politiet som ledd i etterforskingen etter strpl. § 230, er det et åpent spørsmål om det kan innfortolkes et krav til vitneplikt etter § 108 ved anvendelse av § 118. Bakgrunnen for spørsmålet er at § 230 fjerde ledd forutsetter at § 118 første og annet ledd vil gjelde tilsvarene og at det av den grunn også foreligger et ulovfestet konkretiseringskrav som det er antatt at det vil gjøre ved bruk av § 108. Dette kravet forutsetter at politiet må vise til at det er satt i gang etterforsking om bestemte straffbare forhold. Kravet innebærer ikke at det er nødvendig at en bestemt person er siktet eller mistenkt, men at forholdet det søkes utlevert informasjon om er konkretisert i tilstrekkelig grad. [65]

Etterforsking iverksettes og utføres av politiet, jfr. strpl. § 225 første ledd, og foretas når det som følge av anmeldelse eller andre omstendigheter ”er rimelig grunn til å undersøke om det foreligger straffbart forhold”, jfr. § 224 første ledd. Etterforskingskravet vil sjelden by på problemer, da politiet i de aller fleste tilfeller vil ha satt i gang etterforsking når de søker trafikkdata.

Problemet ved bruk av bestemmelsen oppstår først ved vurderingen om det er vist til ”bestemte straffbare forhold”. PT - som mener at dette er et strengt krav - ba i brev til Justisdepartementets lovavdeling av 8.2.2008 om en prinsipputtalelse hva gjelder dette spørsmålet. I sitt svar av 10.2.2009 kommer det klart frem at lovavdelingen ikke deler PT sitt standpunkt om at det gjelder samme krav til konkretisering både ved bruk av § 230 og § 118, jfr. § 108.

---

[64] http://www.npt.no

[65] Bjerke/Keiserud s. 447 om strpl. § 108

Lovavdelingen uttaler at selv om § 230 henviser til § 118 i sitt fjerde ledd innebærer dette ikke at: *"hovedregelen om vitneplikt etter straffeprosessloven § 108, og dermed den tilhørende konkretiseringskravet gjelder fullt ut også ved forklaringer til politiet."*

Lovavdelingen går så inn på en drøftelse om hvorfor reglene er og bør være annerledes ved forklaringer for politiet. Det legges vekt på at politiforklaringer *"ofte gis på et tidlig stadium i en straffesak, og ikke sjelden vil bevisbildet være mangelfullt eller uklart."*

Forskjellen blir videre forklart med at det ved forklaring til politiet ofte vil ha som funksjon å *"avklare behovet for ytterligere etterforskning, eventuelt i hvilken retning etterforskingen skal gå."*

Lovavdelingen konkluderer med at et slikt krav vil "*innebære at politiet aldri kan få samtykke til opphevelse av taushetsplikten etter straffeprosessloven § 118 med mindre det kan vise til at et bestemt straffbart forhold er under etterforskning. I noen tilfeller kan dette vanskeliggjøre politiets arbeid, ikke minst der saken har et visst hastelement."*

Ut fra det ovennevnte er det klart at Lovavdelingen ikke mener at et konkretiseringskrav ved bruk av § 230 skal gjelde "fullt ut". Hva som menes med "fullt ut" er uklart, men mye tyder på at kravet ikke er like strengt som ved bruk av § 118 og at politiet her er gitt en større undersøkelsesadgang ved bruk av § 230.

Dersom PT nekter å gi fritak fra taushetsplikten kan politiet angripe vedtaket ved kjennelse fra retten etter § 118 annet ledd, jfr. § 230 fjerde ledd. Domstolen skal da etter § 118 annet ledd foreta en avveining mellom "hensynet til taushetsplikten og hensynet til sakens opplysning." Følgene av at domstolen dømmer i politiets favør og gir fritak fra taushetsplikt er at teleoperatøren får plikt til å forklare seg overfor politiet, jfr. § 118, jfr. § 230 fjerde ledd.

Dersom PT fritar fra taushetsplikt etter anmodning fra politiet vil det være opp til tilbyder om denne adgangen skal benyttes. Ingen kan etter § 230 pålegges forklaring til politiet (med mindre det foreligger rettslig kjennelse - da vil forklaringen regnes som forklaring overfor retten). Den strenge vitneplikten vil kun gjelde overfor retten etter § 108, jfr. § 118. Tilbyderen kan derimot velge å avgi frivillig forklaring til politiet etter § 230.

I et brev til Ombudsmannen i 2006 uttaler Justisdepartementet at det fremstår som *"uheldig at trafikkdata utleveres dels som frivillig vitneforklaring, dels som beslag/utlevering, blant annet av hensyn til den som har krav på hemmelighold.* Departementet mener at sakene for fremtiden bør følge tvangsmiddelsporet i strpl. fordi en slik fremgangsmåte vil gi bedre rettssikkerhet.

På grunn av usikkerheten rundt dette kravet, samt at frivillig forklaring kan virke uheldig inn på rettssikkerheten til de som berøres av utlevering, er flere tilbydere forsiktige med å "forklare" seg på denne måten til politiet etter fritak fra PT. Dette støttes også av NOU 2009:15 hvor det opplyses om at flere teletilbydere krever at påtalemyndigheten fatter beslutning om beslag etter strpl. § 203, jfr. § 205, eller at det blir fattet rettslig beslutning om utleveringspålegg i henhold til strpl. § 210.[66]

4.4.3 Beslag etter strpl. § 203 eller utleveringspålegg etter strpl. § 210

4.4.3.1 Innledning

Noen plikt til å utlevere trafikkdata for tilbyder foreligger som nevnt ikke før det er tatt i bruk et straffeprosessuelt tvangsmiddel. Når politiet skal få utlevert trafikkdata fra en tilbyder vil det naturlige utgangspunktet være strpl. § 203, jfr. § 205 om beslag og § 210 om utleveringspålegg.

[66] NOU 2009:15 s. 217

Både §§ 203 og 210 har samme inngangsvilkår for å kunne tas i bruk. For det første er det et krav at tingen som beslaglegges eller kreves utlevert "må antas" å ha betydning som bevis. Etter praksis fra Høyesterett er det klart at "må antas" setter opp et krav om at rimelig mulighet er nok.[67]

For det andre er det et krav om at det som beslaglegges eller utleveres er en "ting". At trafikkdata kan regnes for å være en "ting" ble enstemmig slått fast av Høyesterett i en kjennelse inntatt i Rt. 1992 s. 904. I kjennelsen fikk påtalemyndigheten medhold i at begjæringen om at det kunne foretas beslag hos Televerket i utskrift av registrerte telefonoppringninger til og fra siktedes mobiltelefon etter § 203 og § 204, jfr. § 210 var gyldig. Høyesteretts Kjæremålsutvalg kom til at begrepet "ting" i § 203 er av generell karakter og at beslagsadgangen og utleveringsplikten ikke bare omfatter legemlige gjenstander, *"men også opplysninger som lagres på data og som i tilfelle må gjøres tilgjengelig ved utskrifter,…"*[68] Utvalget uttaler videre at det ikke finnes holdepunkter for at *"generelle personvernhensyn medfører at registrerte oppringninger fra et bestemt telefonnummer til et annet – når disse har betydning som bevis – faller utenfor straffeprosesslovens alminnelige hjemmel for beslag og utlevering."*[69] Kjennelsen ble fulgt opp i Rt. 1992 s. 928, og Rt. 1997 s.470 som begge omhandler påtalemyndighetens adgang til å hente ut inn og utgående samtaler fra en mobiltelefon.

I tillegg til det ovennevnte, og som nevnt over under punkt 4.4.2, understrekes det at det også foreligger et konkretiseringskrav ved bruk av disse bestemmelsene. Dette støttes av to avgjørelser i Høyesterett inntatt i Rt. 1992 s. 898 og Rt. 1997 s. 266. Bakgrunnen for en slik plikt er først og fremst for at den som plikten retter seg mot skal ha mulighet til å vite hva som skal fremlegges. Ved meget vidtgående utleveringsanmodinger vil personvernet til

---

[67] Rt. 1998 s. 1839, Rt. 1999 s. 1115

[68] Rt. 1992 s. 904 s. 906

[69] Ibid.

en stor gruppe mennesker bli berørt om et slikt konkretiseringskrav ikke foreligger, se bl.a. premissene fra Rt. 1999 s. 1944, samt RG. 2006 s. 811.

Det fremgår av bestemmelsenes ordlyd at de kan fremsettes mot andre enn den mistenkte, jfr. annet punktum i § 203, samt ordet ”besitteren” i § 210 første ledd.

Historisk sett har de to bestemmelsene gjennomgått små endringen om man sammenligner med andre bestemmelser i lovverket. § 203 for eksempel har i stor grad hatt samme ordlyd i over 100 år. I 1887 hadde bestemmelsen, som da var inntatt i lov om rettergangsmåter i straffesaker § 212, følgende ordlyd:

> *”Ting er antages at være af betydning som Bevismidler eller at burde kjennes forbudte, kan beslaglegges.”*

Selv om ordlyden i bestemmelsen har forandret seg lite, har domstolene alltid tolket bestemmelsen i takt med tiden og i henhold til den teknologiske utviklingen.[70]

4.4.3.2 Beslag etter strpl. § 203

Etter § 205 første ledd er det påtalemyndigheten som beslutter at det skal foretas beslag etter § 203, eventuelt polititjenestemann etter § 206. Beslutningen skal så vidt mulig være skriftlig og opplyse om: ”hva saken gjelder, formålet med beslaget og hva det skal omfatte.”, jfr. § 205 første ledd annet punktum.

Vitneproblematikken som oppstilles i § 204 ble omtalt under punkt 4.4.2 i avhandlingen og vil ikke bli nevnt mer inngående i det følgende.

Det er etter Høyesterettspraksis lagt til grunn at det skal leses inn et krav til ”skjellig grunn til mistanke” for at en straffbar handling er begått før man kan ta beslag i ”ting” etter § 203.

---

[70] Se bl.a. Rt. 2009 s. 1011 hvor ”ting” etter § 203 også omfatter domenenavn.

Dette kommer bl.a. frem av Rt. 1998 s. 1839 hvor førstvoterende enig i lagmannsrettens lovtolkning av bestemmelsen og at *"en ting antas å kunne ha betydning som bevis eller å kunne inndras, innebærer at rimelig mulighet er nok. Det kreves altså ikke så mye som skjellig grunn. Derimot må det være skjellig grunn til mistanke om at en straffbar handling er begått for at beslag kan finne stred etter § 203."*[71]

Kravet om skjellig grunn til mistanke vil si at det må være mer sannsynlig at vedkommende har begått handlingen enn at han ikke har det, med andre ord kreves det sannsynlighetsovervekt for skyld.[72]

På grunn av de forholdsvis strenge kravene som oppstilles i § 203 vil det sjelden være aktuelt å bruke bestemmelsen hvor politiet ikke har en sterk sak mot den mistenkte.[73]

For å kunne beslaglegge en "ting" etter § 203 er det en forutsetning har man har tilgang til tingen som skal beslaglegges. Som nevnt vil trafikkdata som søkes beslaglagt være i tilbyderens besittelse og § 203 vil derfor stort sett alltid brukes sammenholdt med § 205 første ledd hvor beslaget kommer som en beslutning fra påtalemyndigheten, eventuelt sammen med § 210 om utleveringspålegg.

Beslag av ting som besitteren ikke vil utlevere frivillig besluttes av påtalemyndigheten, jfr. § 205 første ledd. Dersom særlige grunner foreligger kan spørsmålet om beslag forlegges retten for beslutning, jfr. § 205 annet ledd. Bestemmelsen har ved bruk av annet ledd de samme vilkår for å kunne brukes som første ledd og krever at det som søkes utlevert er konkretisert. I tillegg er det et krav om at beslutningen leses opp eller forevises den som beslutningen retter seg mot, jfr. strpl. § 200 første ledd. Dette er en forutsetning når politiet vil ta beslag i trafikkdata, da det er tilbyderen som er i besittelse av tingen som kan ha

---

[71] Rt. 1998 s. 1839 s. 1840

[72] Rt. 1993 s. 1302

[73] NOU 1997:15 s. 61

betydning som bevis. I tillegg gjelder strpl. § 209 og § 208 første og tredje ledd tilsvarende. Etter § 208 første ledd skal påtalemyndigheten sørge for at den som rammes av beslaget skal gjøres kjent med muligheten for å bringe beslaget inn for retten med spørsmål om det skal opprettholdes. Et relevant spørsmål vedrørende denne plikten vil være om også den mistenkte rammes av bestemmelsen når beslaget kun retter seg mot det tilbyderen besitter.

Det er uttalt av Metodeutvalget i NOU 1997:15 s. 68 at alle som har en "aktuell interesse" i den beslaglagte ting skal varsles. Hvem som rammes skal her følge de samme rammene som stilles opp i strpl. § 377 om kjæremålsadgang. Utvalget understreker også at *"mistenkte vil imidlertid ofte rammes av utleveringspålegget og derved ha krav på underretning."*[74] Det samme blir forutsatt i Ot.prp.nr. 64 (1998-1999) s. 106 hvor det kommer frem at den som rammes av beslag eller utleveringspålegg skal underrettes om dette, jfr. §§ 200, 208, jfr. 205 første ledd siste punktum og § 210.

Det er etter dette relativt klart at dersom politiet anvender §§ 203, jfr. 205 ved beslag av trafikkdata må vedkommende, da også mistenkte, varsles om dette, jfr. § 208. Unntak fra dette følger av § 208a. Bestemmelsen hjemler utsatt underretning om noen med skjellig grunn mistenkes for handling eller forsøk på handling som etter loven medfører høyere straff enn fengsel i 6 måneder. Utsatt underretning gjelder overfor "den mistenkte", men også "andre som rammes av beslaget." I tillegg til straffekravet krever bestemmelsen også at "det er strengt nødvendig for etterforskingen i saken at underretning ikke gis." Det er i Ot.prp.nr. 64 (1998-1999) uttalt at det skal *"mye til før underretning kan utsettes."*[75] Ordlyden og reelle hensyn tilsier at sondringen her bør gå hvor underretningen med all sannsynlighet vil vanskeliggjøre eller forspille sentrale elementer i etterforskingen.

---

[74] NOU 1997:15 punkt 6.5.4

[75] Ot.prp.nr. 64 (1998-1999) s. 151

Ved bruk av § 208a vil retten oppnevne en offentlig advokat for den mistenkte. På denne måten har lovgiver søkt å oppfylle deler av rettighetsregisteret til den som utsettes for et slik beslag uten å bli underrettet om det.

4.4.3.3 Strpl. § 210

Etter § 210 første ledd kan retten pålegge en tilbyder å utlevere trafikkdata såfremt tilbyderen "plikter å vitne i saken" (se punkt 4.4.2 om dette). At ingen plikter til å bidra til egen domfellelse etter blant annet strpl. § 90 og 91 tilsier at bestemmelsen ikke kan brukes mot den som selv er misstenkt. Dersom den mistenkte selv besitter tingen må derfor politiet her gå gjennom § 203, jfr. § 205.

Ser man annet ledd sammenholdt med første ledd kan det virke som om retten her skal fatte utleveringspålegget ved kjennelse, jfr. "tre istedenfor rettens kjennelse" i annet ledd. Dette stemmer ikke overens med forutsetningene i forarbeidet og sammenhengen i lovverket. Av den grunn ble bestemmelsens annet ledd foreslått endret av metodeutvalget i NOU 2009: 15 s. 370 til *"tre istedenfor beslutning av retten."*

Om man også skal tolke inn et krav om skjellig grunn til mistanke om en straffbar handling er begått i § 210 er et åpent spørsmål. Flere momenter i ordlyden taler for å ikke tolke inn et slikt krav inn i § 210. For det første retter bestemmelsen seg mot den som "besitter" en "ting som antas å ha betydning som bevis". Når en tilbyder besitter tingen har ikke den mistenkte rådigheten over tingen og at politiet da vil få utlevert tingen vil ikke være et like inngripende tvangsmiddel som å kreve tingen utlevert fra den som anses å eie tingen. Dette poenget ble i Ot.prp.nr. 64 (1998-1999) på side 101 illustrert ved at det ved bruk av § 210 forutsettes at *"besitteren må da medvirke aktivt for at politiet skal få hånd om tingen – i motsetning til ved beslag hvor politiet kan skaffe seg tingen uten besitterens medvirkning."*

For det andre vil kravet til "skjellig grunn" bli kontrollert av PT ved fritak fra taushetsplikten. Uansett vil strpl. § 170a vil komme inn som skranke ved bruk av bestemmelsen og da foreta en forholdsmessighetsvurdering.

For det andre vil det for politiet i flere situasjoner være av essensiell verdi å kunne avkrefte eller forsterke sine mistanker ved å hente inn trafikkdata ved hjelp av § 210. At man først da må sannsynligere overvekt av sannsynlighet for at det er begått et straffbart forhold vil da undergrave mye av bestemmelsens virkeområde sett fra et etterforskingsperspektiv.

Det som taler for å tolke et krav om skjellig grunn til mistanke om at en straffbar handling har funnet sted inn i bestemmelsen, er for det første det at § 210 uten et slikt tilleggsvilkår vil få et meget vidt anvendelsesområde, i og med at bestemmelsen ikke innholder noe kriminalitetskrav. Utvalget i NOU 2004:6 uttaler at det ved vurderingen av personvernet og bruk av § 210 vil være et problem, og at *"det er betenkelig i seg selv å ha bestemmelser med en slik rekkevidde."*[76] Jeg er langt på vei enig i utvalgets sondring her. Uten et krav til "skjellig grunn" vil bestemmelsen kunne brukes i forebyggende øyemed der politiet kun har svake mistanker om straffbare forhold. Sammenhengen i straffeprosessloven kapittel 16 tilsier etter min mening at en slik mulighet ikke foreligger.

For det andre er § 203 og § 210 utstyrt med samme inngangsvilkår for å kunne tas i bruk, og likheten mellom de to bestemmelsene er påfallende. Likheten og sammenhengen i lovverket vil derfor tale for at et slikt krav også må leses inn i § 210. Denne sammenhengen i lovverket støttes også av ordlyden i § 215a som hjemler sikring av elektroniske lagrede data. Etter bestemmelsens annet ledd er mistankekravet "grunn til å tro at det er begått en straffbar handling". Inngangsvilkåret i bestemmelsens første ledd krever at sikringspålegget omfatter data "som antas å ha betydning som bevis" – altså samme vilkår som ved bruk av § 203 og § 210. Departementet har i sin vurdering av § 215a i Ot.prp.nr. 40 (2004-2005) kommet til at bestemmelsen ville miste sin betydning om kravet til skjellig grunn også skal leses inn i denne. Dette begrunnes i at *"dersom mistanken først er så sterk, må det antas at politiet normalt vil foretrekke å beslaglegge de aktuelle dataene i medhold av straffeprosessloven § 203 eller kreve dem utlevert i medhold av straffeprosessloven §*

[76] Punkt 7.12.4.1

210".[77] Uttalelsen fra departementet taler for at et krav om skjellig grunn også må tolkes inn i § 210.

At bestemmelsen regnes for å være et straffeprosessuelt tvangsmiddel setter legalitetsprinsippet og personvernet i en sterk posisjon ved vurderingen om et krav til skjellig grunn skal leses inn i § 210.

Etter en avveining mellom de ovennevnte momentene vil det etter min vurdering være naturlig å tolke inn et krav til skjellig grunn til mistanke om at en straffbar handling er begått når retten skal pålegge besitteren å utlevere trafikkdata som kan ha betydning som bevis etter § 210 første ledd.

Etter § 210 annet ledd første punktum kan ordre fra påtalemyndigheten tre istedenfor kjennelse (beslutning) av retten dersom det ved opphold er fare for at etterforskingen vil lide. Påtalemyndighetens beslutning skal da forelegges retten for godkjennelse snarest mulig, jfr. § 210 første ledd annet punktum.

Etter § 210a kan retten ved kjennelse mot den som med skjellig grunn mistenkes for handling eller forsøk på handling som etter loven kan medføre høyere straff enn fengsel i 6 måneder utsette underretting dersom dette er strengt nødvendig for etterforskingen. Bestemmelsen sammenfaller her med kravene som oppstilles i § 208a ved utsatt underretning. Kravet til strengt nødvendig vil si, som nevnt under punkt 4.4.3.2, at det skal *"mye til før slik tillatelse kan gis"*[78] En vurdering av dette kriteriet ble utført av Metodeutvalget i NOU 2009:15, da etter den likelydende bestemmelsen i § 200a. Utvalget konkluderer med at underretningen da må være *"av vesentlig skade for etterforskingen"*[79]

---

[77] Ot.prp.nr. 40 (2004-2005) s. 26

[78] Ot.prp.nr. 64 (1998-1999) s. 147

[79] NOU 2009:15 s. 175

Ved bruk av § 210a som ved bruk av § 208a vil den mistenkte da få oppnevnt en offentlig forsvarer etter § 100a som vil ivareta hans interesser.

§ 210 kan ikke brukes for data som tilbyderen ”vil få besittelse av”, jfr. § 210b. Det som avhandlingen under punkt 4.3.4.3 definerer som fremtidige trafikkdata. For å få utlevert slike data kreves rettens kjennelse, samt skjellig grunn til mistanke for en handling eller forsøk på handling som kan medføre straff i form av fengsel i 5 år eller mer, eller som rammes av straffeloven §§ 90, 91, 91a, 94, jfr. 90, jfr. § 210b første ledd. § 210b ble tilføyd ved lov av 3. desember 1999 nr. 82 og innsnevret adgangen til å utgi trafikkdata fremover i tid. En slik adgang ble først fastsatt av Høyesterett i Rt. 1997 s. 470, men altså endret ved lovendringen. Et slikt pålegg kan bare gis for et bestemt tidsrom som ikke skal vare lenger enn strengt nødvendig, og ikke lenger enn 4 uker om gangen, jfr. § 210 b annet ledd.

Etter bestemmelsens siste ledd vil § 210b ikke kunne brukes ved utlevering av fremtidige kommunikasjonsdata. Utlevering av slike data hjemles kun etter § 216b annet ledd bokstav d. § 210b siste ledd viser til bokstav c i § 216, men dette er en feil som oppsto ved revisjon av bestemmelsen i 2005 hvor bokstav c ble endret til bokstav d. § 210b siste ledd skal åpenbart vise til bokstav d i § 216b.

4.4.3.4 Sikringspålegg etter strpl. § 215a

Trafikkdata blir hos tilbyderne slettet etter alt fra 3 uker til 5 måneder avhengig av hva som genererer dataen (internettrafikk eller mobiltelefoni) og faktureringsrutiner (se punkt 4.3.5). Det fremgår av ekoml. § 2-7 annet ledd at så snart at dataen ikke lenger er nødvendig for kommunikasjons- eller faktureringsformål skal de slettes eller anonymiseres (se punkt 4.3.5). Dette gir åpenbare utfordringer for politiet i en etterforskingssituasjon ved at nødvendige data kan bli slettet hos tilbyderne. Som ledd i etterforskingen kan derfor påtalemyndigheten etter § 215a første ledd: ”gi pålegg om sikring av elektronisk lagrede data som antas å ha betydning som bevis.” Det kommer frem av Ot.prp.nr. 40 (2004-2005) s. 26 at bestemmelsen er å regne for et straffeprosessuelt tvangsmiddel og de ovennevnte vurderingene hva gjelder § 203 og § 210 vil gjelde tilsvarende.

Bestemmelsen ble til som en inkorporering av artikkel 16 i Europarådets konvensjon om datakriminalitet ved lov av 8. april 2005 nr 16. Konvensjonen ble utarbeidet som et samarbeid mellom flere nasjoner for å tilpasse straffe- og straffeprosesslovgivningen i kjølevannet av den teknologiske utviklingen og for å få effektive hjelpemidler mot den nye grenseoverskridende kriminaliteten, særlig på IKT-området.

Det kommer frem av Ot.prp.nr. 40 (2004-2005) at bestemmelsen med ”sikring” mener *”ethvert tiltak som ivaretar de aktuelle dataenes integritet, tilgjenglighet og autentisitet.”*[80] Dette kan skje ved at tas kopi av relevante data, eller at det som sikres gjøres utilgjengelige for andre enn de pålegget retter seg mot. Sikringspålegget kan kun rette seg mot det som avhandlingen kaller historiske data.[81] Et sikringspålegg gjelder ikke fremover i tid, slik tilfellet er ved beslutning om kommunikasjonskontroll etter strpl. § 216a og § 216b.

Begrepet ”grunn til å tro” i annet ledd krever ikke sannsynlighetsovervekt for at en straffbar handling er begått, men det kreves at mistanken bygger på *”visse objektive holdepunkter i det konkrete saksforholdet, og kan derfor ikke utelukkende forankres i rent subjektive forestillinger.”*[82] Kravet til om det er begått en straffbar handling er ved bruk av bestemmelsen derfor lavere enn det som følger av § 203 og § 210.

Sikringspålegget etter bestemmelsens tredje ledd kan kun gjelde for et ”bestemt tidsrom” og ikke lenger ”enn nødvendig” og ”høyst 90 dager om gangen.” Om sikringen av dataene skal opprettholdes kan prøves av retten, jfr. § 215a fjerde ledd og henvisningen til § 208 første og tredje ledd.

---

[80] Ot.prp.nr. 40 (2004-2005) s. 5 og s. 27

[81] Ibid. s. 22

[82] Ibid s. 36

Mistenkte skal underrettes om pålegget straks dataene er sikret og han får status som siktet i saken, jfr. § 215a tredje ledd annet punktum. I dette ligger det et krav om underretting når påtalemyndigheten har erklært ham for siktet, når forfølging mot ham er innledet ved retten eller når det er besluttet eller foretatt pågripelse, ransaking, beslag eller lignende tvangsmidler mot ham, jfr. strpl. § 82 første ledd.[83]

Ved sikringspålegg mot andre enn den mistenkte, skal underretning gis straks pålegget er gjennomført, jfr. "før øvrig" i § 215a tredje ledd siste punktum.[84] Dette betyr at vitner som den mistenkte har vært i kontakt med skal gis underretning om sikringspålegget så snart det gjennomføres. Denne varslingsplikten for påtalemyndigheten kan gjøre etterforskingssituasjonen vanskeligere ved at personer i den mistenktes krets får melding om at et slikt tvangsprosessuelt skritt er anvendt. Dette er søkt avhjulpet med henvisningen til § 216i i § 215a fjerde ledd siste punktum, hvor det kommer frem at alle skal bevare taushet om at det er begjært eller besluttet kommunikasjonskontroll. Etter § 216i første ledd annet punktum gjelder det samme "andre opplysninger som er av betydning for etterforskningen, og som de blir kjent med i forbindelse med kontrollen eller saken."

Det er grunn til å påpeke at bestemmelsen ikke vektlegger hensynet til etterforskingen når den krever en slik varslingsplikt til vitner og andre som blir berørt av sikringspålegget. Dette kan være personer som gjerne er i den mistenktes nærmeste krets, med tanke på at det har vært telefonisk eller nettbasert kontakt mellom dem. At taushetsplikt bestemmelsen i § 216i da brukes overfor den et slikt sikringspålegg retter seg mot skal ivareta hensynet til etterforskingen på en adekvat måte er vanskelig å tenke seg, spesielt der hvor man etterforsker et kriminelt nettverk eller en kriminell organisasjon.

Bestemmelsen virker mindre gjennomtenkt enn for eksempel § 203 og § 210 som har bestemmelser som hjemler utsatt underretning. Dersom politiet da først velger å bruke den

---

[83] Ibid s. 35

[84] Kommentarutgaven til straffeprosessloven av Geir Sunde Haugland (note 1474)

mindre inngripende bestemmelsen i § 215a for å sikre trafikkdata vil politiet være tvunget til å gi andre som rammes av sikringspålegget melding om tiltaket.

Etter § 215a femte ledd gir den som pålegget retter seg mot plikt til å utlevere nødvendige trafikkdata for å kunne spore opp "hvor dataene som omfattes av sikringspålegget kom fra og hvor de eventuelt ble sendt til". Utleveringsplikten omfatter her kun trafikkdata og kun de dataene som kan bidra til å spore en bestemt kommunikasjonsoverføring.[85]

4.4.4 Strpl. § 216b

4.4.4.1 Bestemmelsens historiske utvikling

Kapittel 16a om kommunikasjonskontroll ble først en del av straffeprosessloven ved lovendring av 5 . juni 1992 nr. 52. Da hjemlet bestemmelsene kun kommunikasjonskontroll i narkotikasaker og var i stor grad inkorporert i straffeprosessloven for å ta over for midlertidig lov av 17. desember 1976 nr. 99 som da hjemlet kommunikasjonskontroll ved narkotikakriminalitet.

Ved lovendingen i 1992 fikk § 216b følgende ordlyd:

> *"Finner retten skjellig grunn til mistanke om en handling som nevnt i § 216 a første ledd, kan retten ved kjennelse beslutte at ekspidering av samtaler til eller fra bestemte telefoner som den mistenkte besitter eller kan ventes å ville bruke, skal innstilles eller avbrytes. Videre kan retten ved kjennelse beslutte at telefonen skal stenges for samtaler eller at styrer av telefonsentral skal gi politiet opplysninger om hvilke telefoner som i et bestemt tidsrom skal settes eller har vært satt i forbindelse med en bestemt telefon."*

[85] Ot.prp.nr. 40 (2004-2005) s. 35

For at § 216b skulle komme til anvendelse etter 1992 loven var det en forutseting at handlingen den mistenkte hadde utført eller forsøkte å utføre ville rammes av straffeloven § 162 eller § 317 § 162, jfr. § 216a første ledd (1992). Det forelå derfor de samme inngangsvilkår som ved bruk av datidens § 216a som hjemlet kommunikasjonsavlyttning i alvorlige narkotikasaker og i saker om rikets sikkerhet.[86] I tillegg hjemlet bestemmelsen kun informasjonsutlevering og kontroll med kommunikasjon som omhandlet telefoner.

Ved lovendring av 3. desember 1999 ble § 216b i all hovedsak gitt til den ordlyd vi har i dag. Lovendring ble i stor grad begrunnet i ønsket om å utvide dens anvendelsesområde ved å hjemle bruken av bestemmelsen i straffekrav og ikke i forbryterkrav. Etter Metodeutvalgets vurdering i NOU 1997:15 ble det foreslått at straffekravet i § 216b kun skulle være 3 år. Det ble ved denne vurdering av strafferammen lagt vekt på at kontroll med trafikkdata er et betydelig inngrep i den personlige rettssfære, men lang mindre enn informasjon om kommunikasjonens innhold.[87] Departementet er langt på vei enig med Metodeutvalget, men faller ned på et straffekrav på 5 år, da dette må være ønskelig strafferamme i forhold til den kriminalitet som § 216b ønsker å omfatte.

Endringene i § 216b ble også begrunnet i nye og mer teknologiske muligheter for politiet i sin kriminalitetsbekjempelse, samt at de kriminelle også i stor grad hadde begynt å utføre kriminalitet som etterlater elektroniske spor som nå kunne undersøkes ved bruk av § 216b. Det at man ved lovendringen gikk bort fra kravet om at kommunikasjonskontrollen kun gjaldt telefoner var også en utvidelse som i stor grad var begrunnet i den teknologiske utviklingen og mulighetene man hadde fått gjennom datamaskiner og andre kommunikasjonsanlegg.

---

[86] Ot.prp.nr. 64 (1998-1999) s. 158

[87] NOU 1997:15 punkt 6.2.3

4.4.4.2 Bruk av § 216 ved utlevering av trafikkdata

Etter strpl. § 216b kan retten ved kjennelse gi politiet adgang til å foreta ”annen kontroll” om noen med ”skjellig grunn” mistenkes for handling eller forsøk på handling som kan medføre straff av fengsel i 5 år eller mer etter bokstav a, eller som rammes av en av straffebestemmelsene som oppstilles i bokstav b.

Hva som ligger i begrepet ”annen kontroll” fremkommer av bestemmelsens annet ledd og omfatter blant annet, etter bokstav d, ”at eier eller tilbyder av nett eller tjeneste som benyttes ved kommunikasjonen skal gi politiet opplysninger om hvilke kommunikasjonsanlegg som i et bestemt tidsrom skal settes eller har vært satt i forbindelse med anlegg som nevnt i bokstav a, og andre data knyttet til kommunikasjon.” Med ”anlegg som nevnt i bokstav a” menes ”bestemte telefoner, datamaskiner eller andre kommunikasjonsanlegg som den mistenkte besitter eller antas å ville bruke”, jfr. § 216b annet ledd, bokstav a. Ordlyden i bestemmelsen forutsetter at kommunikasjonsanlegget er identifisert, jfr. ”bestemte” og at den mistenkte besitter eller antas å ville bruke kommunikasjonsanlegget. Kravene som her stilles opp gjør at dersom politiet er usikre på en persons eller kommunikasjonsanleggs identitet kan bestemmelsen ikke anvendes. Dette blir understreket av Høyesteretts kjæremålsutvalg i kjennelsen inntatt i Rt. 2009 s. 394, nevnt i punkt 2.6 ovenfor.

At bestemmelsen gjelder både for historiske trafikkdata og fremtidige trafikkdata kommer frem av ordlyden i bokstav d, jfr. ”skal settes” og ”har vært satt i forbindelse med”.

Etter § 216f første ledd kan kommunikasjonskontrollen kun gjelde for et ”bestemt tidsrom”. Denne perioden er i utgangspunktet begrenset til fire uker, jfr. § 216f første ledd annet punktum, men kan gis for inntil 8 uker om gangen ved overtredelse av straffeloven kapittel 8 eller 9 om etterforskingens art eller andre særlige omstendigheter tilsier at fornyet prøving etter 4 uker vil være betydningsløst, jfr. § 215f første ledd siste punktum.

Høyesteretts kjæremålsutvalg ble i kjennelsen inntatt i Rt. 2005 s. 194 forelagt spørsmålet om hvilken betydning denne fire ukers tidsbegrensningen har for politiets tillatelse til å få opplysninger om telefonforbindelser i et bestemt tidsrom forut for en begjæring om telefonkontroll. Politiet hadde her fått samtykke av forhørsretten til å avlytte en mistenkts telefon fire uker frem i tid, men ikke til å foreta sporing og nummerregistrering av den mistenktes telefon fire uker bakover i tid. Kjennelsen ble anket til Lagmannsretten som forkastet anken. Utvalget i Høyesterett kom til at både forhørsretten og lagmannsretten hadde tolket loven feil og at *"tidsbegrensningen i § 216f første ledd ikke kan være til hinder for at politiet gis tillatelse til å få opplysninger for et bestemt tidsrom forut for begjæringen selv om det samtidig gis tillatelse for telefonavlytting og nummerregistrering for inntil fire uker fremover i tid."* Det er kun tillatelsen gyldighetstid i seg selv som *"ikke kan overstige fire uker."* Selv om kjennelsen ble avsagt i 1995 og gjaldt den gamle § 216f (1992) er det ikke foretatt endringer i bestemmelsen som tilsier at den skal tolkes annerledes.

I tillegg til mistankekravet og straffekravet i § 216b første ledd oppstiller § 216c et krav om at tillatelse til kommunikasjonskontroll bare kan gis om det vil være "av vesentlig betydning" for oppklaring av saken, og at oppklaring "ellers i vesentlig grad vil bli vanskeliggjort." Det følger av bestemmelsens annet ledd at det må foreligger "særlige grunner" for at tillatelse til kommunikasjonskontroll kan gis om den telefon den mistenkte antas å ville bruke også kan brukes av flere personer. For utlevering av trafikkdata er dette kravet avhjulpet noe i § 216b annet ledd bokstav a som krever at kommunikasjonsanlegget er i den mistenktes besittelse eller er noe han antas å ville bruke.

Etter § 216d kan ordre fra påtalemyndigheten tre istedenfor kjennelse fra retten. Kravet er da at det er "stor fare for at etterforskningen vil lide". Bestemmelsen forutsetter da at påtalemyndighetens beslutning så snart som mulig og "senest 24 timer etter at kontrollen ble begynt", forelegges retten for godkjennelse.

Enhver skal på begjæring gis underretning om bruk av § 216b, jfr. § 216j. Med enhver menes kun enhver som er mistenk i saken.[88] Innehaveren av en telefon som omfattes av det som hentes ut etter § 216b vil derfor ikke være omfattet så lenge han ikke er mistenkt i saken. Etter § 216j annet ledd kan underretning gis tidligst ett år etter at kontrollen er avsluttet. Etter § 216j tredje ledd kan retten ved kjennelse bestemme at underretning skal unnlates eller utsettes over et nærmere fastsatt tidsrom om "det vil være til skade for etterforskingen at underretning gis." Unnlatelsen er tenkt som en sikkerhet om etterforskingen fortsatt pågår ett år etter at kontrollen er avsluttet, jfr. Ot.prp.nr. 40 (1991-1992) s. 43.

Som ved bruk av de andre tvangsmidlene vil den mistenktes rettigheter følges opp av offentlig oppnevnt advokat etter strpl. § 100a.

Etter § 216h første ledd skal kontrollutvalget føre etterfølgende kontroll med saker som etterforskes ved bruk av § 216b. Dette er tenkt som en ekstra sikkerhet for den som berøres av kontrollen.

På grunn av de strenge materielle kravene til å bruke bestemmelsen blir den som oftest brukt i samband med § 216a når man er avhengig av trafikkdata. Andre tilfeller der bestemmelsen gjerne blir brukt er når politiet ønsker fortløpende utlevering av trafikkdata eller hvor man ønsker å holde kontrollen hemmelig over lengre perioder enn det § 208a eller § 210a hjemler. [89]

4.4.5 Utlevering ved samtykke

Samtykke fra abonnenten vil være den minst inngripende måten å få utlevert trafikkdata på. Dette fremkommer av ordlyden i ekoml. § 2-9 første redd hvor taushetsplikten ikke gjelder overfor "andre enn de som opplysningene gjelder."

---

[88] Bjerke og Keiserud s. 762

[89] NOU 2009:15 s. 217

Da behandling av trafikkdata faller inn under personopplysningsloven, jfr. persl. § 2 nr. 1, jfr. § 3a, må samtykke være gitt etter lovens § 2 nr. 7 (se punkt 4.3.5).

Bruken av samtykke som utleveringsgrunn er ikke alltid praktisk for politiet. Det krever for det første at etterforskingen blir avslørt overfor den mistenkte. En annen begrensning vil være at den som blir etterforsket ikke vil hjelpe politiet i saken mot ham selv. Av den grunn blir samtykke som oftest brukt hvor offeret selv henvender seg til politiet, eller der politiet vil etterforske en persons handlingsmønster før en aktuell hendelse, som for eksempel i minuttene før en bilkollisjon.

4.4.6 Nødrett som utleveringsgrunnlag

Nødrettsbestemmelsen i straffeloven § 47 gir politiet muligheten til å til å pålegge tilbyder – uten rettens kjennelse eller PTs fritak fra taushetsplikten – å utlevere trafikkdata for å redde "nogens Person eller Gods fra en paa anden Maate fra en uafvendlig fare." Faren må etter bestemmelsen avveies opp mot den skade som utlevering av trafikkdata kan forvolde, sett opp mot den skade som kan oppstå ved at informasjonen ikke leveres ut.

Nødrett kan for eksempel brukes der hvor personer poster anonyme selvmordstrusler på internett, i forsvinningssaker[90] eller i gissel- eller kidnappingssituasjoner.

Bruk av nødrett forutsetter ingen form for domstolskontroll, verken før eller etter bruken av tvangsmiddelet. Dette kan gi rom for misbruk. At selve bruken er rettstridig, men ikke straffbar taler for en viss form for kontroll i ettertid med tiltaket. Kontrollutvalget for kommunikasjonskontroll (KK) har derfor i sin årlige rapport fra 2009 foreslått at det innarbeides bestemmelser i det relevante lovverket som gir muligheter for en viss domstolskontroll i slike tilfeller.[91]

---

[90] NOU 2004:7

[91] KK rapport 2009 s. 7

Forslaget har mye for seg da flere tilbydere opplyser i rapporten til KK at de føler seg presset til å utlevere taushetsbelagt informasjon når politiet hjemler utlevering i nødrett. Dette selv om tilbyderen ikke kan se at det foreligger en reell nødrettssituasjon.

4.4.7 Vurdering av straffeprosesslovens ordning ved utlevering og beslag av trafikkdata

Som vi har sett ovenfor kan politiet velge flere fremgangsmåter for å få utlever trafikkdata. For det første kan politiet få utlevert trafikkdata frivillig av tilbyder når det er gitt fritak fra taushetsplikten av PT. Dersom tilbyder ikke gir ut informasjonen frivillig kan politiet for det andre bruke beslag- eller utleveringsbestemmelsene i § 203 og § 210. En tredje mulighet er at politiet får utlevert trafikkdata etter § 216b.

Dersom tilbyder velger å gi ut trafikkdata frivillig foreligger ingen regler for varsling av den som berøres av en slik utlevering. Av rettssikkerhetshensyn er det derfor antatt at de fleste tilbydere nå krever at denne informasjonen er underlagt en viss domstolskontroll, da ved bruk av § 203 eller § 210 (se punkt 4.4.2). Det at lovverket stiller opp en frivillig adgang for tilbyderen etter at PT har gitt sitt fritak er i seg selv lite hensiktsmessig – ikke bare på grunn av rettssikkerheten til den som rammes av en slik utlevering, men også på grunn av forutberegnligheten politiet er avhengig av i en etterforskingssituasjon. Som vi har sett ovenfor har det de siste årene vært flere rettsavgjørelser hvor politiet må forholde seg til forskjellig lovverk avhengig av hvilken tilbyder de henvender seg til. Det at tilbyderne også legger seg på forskjellige linjer i forhold til PT sine tolkninger av lovverket kan også gi store problemer for politiet i en presset etterforskingssituasjon, se bl.a. Rt. 1999 s. 1944 hvor dette var tilfellet.

Ved frivillig utlevering er rettssikkerhetshensynet søkt avhjulpet ved at PT foretar en grundig vurdering av momentene som nevnt under punkt 4.4.2 over. Men denne rollen er av PT selv problematisert ved at de stort sett har begrenset tilgang til informasjon vedrørende politiets grunnlag for en slik begjæring, og ofte for lite informasjon til å ta

tilfredsstillende avveininger mellom hensynet til personvernet og etterforskingen. Av rettssikkerhetshensyn mener derfor PT at "frigivelse av historiske trafikkdata bør fattes av domstolene."[92]

Tilbyderen, og i stor grad lovverket, setter i tillegg opp en mulighet for politiet å velge mellom å bruke § 203 eller § 210 for å få utlevert trafikkdata fra tilbyderen. Flere tilbydere godtar at politiet fremsetter beslagsbegjæring etter § 203, jfr. 205, da som oftest ved beslutning av påtalemyndigheten. I senere etterarbeider kan det virke som om departementet har lagt seg på en linje hvor § 210 er den korrekte hjemmelen å anvende ved utlevering av trafikkdata fra en tilbyder. Det er antatt at bestemmelsen gir et bedre vern for rettssikkerheten ved at utleveringen da besluttes av retten, som vil være enda mer uavhengig i forhold til etterforskingssituasjonen enn det påtalemyndigheten vil være.[93] At § 210 har en klarere ordlyd i forhold til utlevering av slike data er åpenbart.

De mange hjemlene for utlevering av trafikkdata har også ført til et system hvor det i visse tilfeller fremkommer en dobbelthjemmel for adgang til informasjonen. Ved utlevering av historiske trafikkdata overfor en som mistenkes for handling som kan gi fengselsstraff i over 5 år eller mer eller som rammes av noen av straffebudene i § 216 b vil politiet kunne bruke både § 216b annet ledd bokstav d og § 210, eventuelt § 205, jfr. § 203, så lenge PT har gitt fritak for taushetsplikten.

Rettighetene til den som berøres av utleveringen vil i stor grad avhenge av hvilken metode politiet her velger å bruke. Dersom politiet går veien om § 210 vil man få en videre adgang til å hente ut trafikkdata ved at bestemmelsen ikke setter opp et krav om "bestemt tidsrom eller "bestemte kommunikasjonsanlegg", jfr. § 216 annet ledd bokstav d.

---

[92] NOU 2009:15 s. 219

[93] Se bl.a. NOU 2009:15 punkt 20.5

Den store forskjellen ved bruk av bestemmelsene ligger i reglene om underretning. Etter § 210a vil retten kunne gi utsatt underretning kun ”dersom det er strengt nødvendig for etterforskingen” (se punkt 4.4.3.3). Ved bruk av § 216b vil underretning om forholdet gis ”tidligst ett år etter at kontrollen er avsluttet”, jfr. § 216j annet ledd. Etter § 216j tredje ledd kan retten ved kjennelse bestemme at underretning unnlates eller utsettes i et nærmere fastsatt tidsrom ”dersom det vil være til skade for etterforskningen at underretning gis, eller andre forhold taler for at underretning bør unnlates eller utsettes”. Fra et underretningssynspunkt vil derfor § 216b gi større muligheter for politiet.

Dobbelthjemmelen blir omtalt av departementet i Ot.prp.nr. 64 (1998-1999) under punkt 13.9. Her blir det uttalt at dobbelthjemmelen er nødvendig fordi beslag- og utleveringsadgangen også hjemler utlevering av andre ”ting” og derfor fungerer de ”selvstendig” og uavhengig av § 216b på flere områder. I tillegg blir det uttalt at det etter departementets syn ikke like betenkelig at det foreligger dobbelthjemmel ved historiske trafikkdata som det vil være for fremtidige trafikkdata, da *”innhenting av historiske data ikke innebærer noen løpende overvåkning av den mistenkte.”*

Denne uoversiktligheten og den nærmest tilfeldige bruken av bestemmelsene som loven her legger opp til må sies å være lite ønskelig med tanke på at utlevering av slike data for det første regnes for å være et straffeprosessuelt tvangsmiddel og for det andre at dataene som leveres ut regnes for å være personopplysninger etter personopplysningsloven. Både legalitetsprinsippet og lovskravet i EMK art. 8 taler for en klarere lovhjemmel. Hensynet til forutberegnlighet, herunder befolkningens adgang til å gjøre seg kjent med lovverket og klargjøre sin rettsstilling taler også for et klarere lovverk.

Flere av de ovennevnte problemstillingene blir også belyst av i NOU 2009:15, hvor PT uttaler at regelverket her bør ”bli mer ensartet.”[94]

[94] NOU 2009:15 s. 219

Metodeutvalget i NOU 2009:15 foreslår flere løsninger vedrørende de ovennevnte problemområdene i lovverket. En av løsningene som oppstilles vil være å stille opp et unntak i § 210 som ikke gir adgang til å bruke bestemmelsen ved utlevering av kommunikasjonsdata, tilsvarende regelen i § 210b siste ledd som unntar for kommunikasjonsdata fremover i tid. Dersom loven endres slik vil imidlertid politiets muligheter bli innsnevret ved at de da ikke får mulighet til å innhente trafikkdata knyttet til andre kommunikasjonsanlegg som den mistenkte besitter eller antas å ville bruke. Utvalget er av den oppfatning at utlevering av trafikkdata ikke er et så kraftig inngrep på personvernet at det er behov for en slik innstramning.[95]

En annen løsningen som oppstilles av utvalget er å endre lovverket, slik at det kun er § 210 flg., som kan brukes ved utlevering av trafikkdata. For at PT sin rolle da skal falle bort, foreslår utvalget at ekoml. § 2-9 første ledd, unntar for taushetsplikt hvor det er lagt frem utleveringspålegg etter § 210.

Sistnevnte forslag har mye for seg. At PT sin rolle blir mer og mer visket ut ved at domstolen uansett vil føre kontroll dersom tilbyderen krever at politiet utferdiger en beslags- eller utleveringsbegjæring etter henholdsvis § 203 eller § 210, taler for en slik adgang. Endringen forutsetter endring i ekoml. § 2-9 fjerde ledd, da endringene i første ledd ikke er ment å omfatte tilbyders vitnemål for retten. Vurderingskriteriet om at det er utilrådelig å etterkomme begjæringen etter fjerde ledd må derfor endres eller falle bort.

Ved bruk av de staffeprosessuelle bestemmelsene vil man i stor grad føre den samme kontrollen som PT foretar i dag, da ved bruk av § 170a. Det at PT sin rolle i stigende grad faller bort tilsier derfor at vi får et lovverk som legger opp til en ren straffeprosessuell prøving av tiltaket politiet foretar seg ved trafikkdatautlevering fra tilbyder. Et mer enhetlig lovverk vil korte ned behandlingstiden og gi forutberegnlighet både for tilbyder, politi og befolkningen generelt.

---

[95] NOU 2009:15. s. 220

5 AVSLUTTENDE BEMERKNINGER OG FREMTIDIGE UTFORDRINGER

Min hovedproblemstilling har vært å vurdere lovverket som politiet og tilbyder av en elektronisk kommunikasjonstjeneste må forholde seg til ved utlevering av identifikasjonsdata eller trafikkdata. Som vi har sett er lovverket uklart, og politiet kan velge flere muligheter for å få utlevert trafikkdata fra tilbydere. Etter min vurdering taler mye derfor for at lovverket gis et klarere og mer enhetlig preg.

Avhandlingen har også søkt å belyse hvordan lovverket er blitt til ved å se på de lovtekniske utviklingslinjene og de rettspolitiske begrunnelsene for de endringene som er blitt gjort. Avhandlingen har på denne måten bl.a. vist at Justisdepartementet har snudd flere ganger i sitt syn på trafikk- og identifikasjonsdata.

At vi i de neste årene kan stå overfor et nytt datalagringsdirektiv vil mest sannsynlig fremskynde prosessen med et nytt og klarere lovverk. Et av direktivets viktigste punkter pålegger landene å gi et regelverk som gjør at trafikkdata blir lagret i minimum seks måneder og maksimalt i to år, da av hensyn til kriminalitetsbekjempelsen. Dette i stor kontrast til lovgivningen vi har i dag, som kun hjemler slik lagring hovedsaklig av hensyn til faktureringsformål - et formål som i stor grad er på vei bort, da flere tilbydere tilbyr fastpris til sine abonnenter. Når det er sagt, og med bakgrunn i de politiske signalene fra de forskjellige partiene på Stortinget ser det ikke ut som om direktivet vil bli vedtatt i nærmeste fremtid.

Uansett, gir direktivet en viktig pekepinn på hvor lovverket er på vei. Internasjonale lovverk kommer til å bli, og er, en viktig brikke i kampen mot nye trusler, som ikke bare truer nasjoner, men hele verdensdeler og levemåter.

Viktigheten av klare og effektive lovverk som blir til etter samarbeid med andre nasjoner er også viktig i forhold til at den moderne teknologien som ikke tar hensyn til landegrenser. Et illustrerende problem oppsto under en nøye planlagt internasjonal politioperasjon kalt ”Operation Sledgehammer” fra 2007. Et grenseoverskridende politisamarbeid førte til at

man fikk innblikk i trafikken gjennom en kroatisk internettside som inneholdt enorme mengder overgrepsbilder. Da de norske IP-adressene ble overlevert politiet var all trafikkdata for denne perioden allerede slettet av tilbyderne. Dette gir et tydelig eksempel på at vi i dag ikke har et lovverk som takler dagens moderne utfordringer.[96]

At lagring av trafikkdata ikke lovlig kan begrunnes av hensyn til politietterforsking er ikke takt med tiden og følger ikke den samme retningen som mange andre land vi liker å sammenligne oss med.[97] Den moderne teknologen har ført til at mye av kriminalitetsbekjempelsen nettopp kan skje gjennom de kanalene oppgaven har fokusert på. At politiet da skal være avskåret fra å bruke denne teknologien så effektivt som mulig, selvfølgelig med passende restriksjoner, kan føre til at Norge faller etter på mange områder når det gjelder etterforsking ved bruk av disse viktige hjelpemidlene.

[96] Høgetveit (2008)

[97] Se bl.a. den Danske rettspleieloven § 786 fjerde ledd som pålegger lagringsplikt i 1 år ”til brug for etterforskning og retsforfølning”.

6 LITTERATURLISTE

Bøker og artikler:

- **Andenæs, Johs**: *"Statsforfatningen i Norge"*, 9. Utgave, Universitetsforlaget, Oslo, 2005.
- **Auglend, Ragnar** m.fl.: *"Politirett"*, 2. utgave, Gyldendal akademisk, Oslo, 2004.
- **Bjerke, Hans Kristian og Keiserud, Erik**: Kommentarer til straffeprosessloven, 3. utgave, Universitetsforlaget, Oslo, 2001.
- **Clemet, Kristin** m.fl.: *"Til forsvar for personvernet"*, Universitetsforlaget, Oslo, 2010.
- **Danielsson, Jerker** m.fl.: *"Elektroniske Spor"*, Norsk Regnesentral, 2005.
- **Hopsnes, Roald**: *"Legalitetsprinsippet"*, Jussens Venner, 2005, s. 77-152.
- **Hov, Jo**: *"Rettergang I"* og *"Rettergang II"*, Papinian AS, Oslo, 2007.
- **Høgetveit, Einar**: *"Lagringsplikt for trafikkdata"*, 2008.
- **Høstmælingen, Njål**: *"Internasjonale menneskerettigheter"*, 2. opplag, Universitetsforlaget, Oslo, 2004.
- **Knoph, Ragnar**: *"Knophs oversikt over Norges rett"*, 12. utgave, Universitetsforlaget, Oslo, 2004.
- **Sunde, Inger Marie**: "*Lov og rett i cyberspace*", Fagbokforlaget, Bergen, 2006.
- **Willassen, Svein**: *"Datalagringsdirektivet – Verdi i etterforskning og risikofaktorer for personvern"*, 2010.

Annet:

- **TV2 Nyhetene**: *"Mener gjengbrødre bestilte drap på Facebook"*, Publisert 19.12.2009 (Sitert: 18.11.2010) http://www.tv2nyhetene.no/innenriks/krim/mener-gjengbroedre-bestilte-drap-paa-facebook-3070741.html

- **Nordberg, Rolf**: *"Drapsforklaring uten en mine"*, Publisert 18.5.2010 (Sitert 18.11.2010). http://www.glomdalen.no/nyheter/article5120932.ece

- **Humlegård, Odd Reidar**: "Datalagringsdirektivet – Høringssvar fra Kripos", Oslo, 12.4.2010.

- **Rønnevig, Leif-Henrik**: Kommentarer til ekomloven. Gyldendal rettsdata. www.rettsdata.no (Sitert 15.10.2010)

- **Haugland, Geir Sunde**: Kommentarer til straffeprosessloven. Gyldendal rettsdata. www.rettsdata.no (Sitert 24.10.2010)

- **Justis- og Politidepartementet**: Prinsipputtalelse vedrørende straffeprosessloven §§ 108, 118 og 230 av 10.2.2009.

Internettsider:

- http://www.internetworldstats.com
- http://www.lovdata.no
- http://www.npt.no
- http://www.regjeringen.no
- http://www.rettsdata.no

Lover:

- Kongeriget Norges Grundlov (Grunnloven) av 17. Mai 1814.

- Lov om Rettergangsmaaden i Straffesager av 7. Januar 1887 nr. 5.

- Lov om Eneret for Staten til Befordring af Meddelelser ved Hjælp av Telegraflinjer og Anlæg av 29. april 1899 (Telegrafloven).

- Almindelig borgelig straffelov (Straffeloven) av 22. mai 1902 nr. 10.

- Lov om rettergangsmåten i straffesaker (Straffeprosessloven) av 22. mai 1981 nr. 25.

- Lov om telekommunikasjon (Teleloven) av 23. juni 1995 nr. 39.

- Lov om politiet (Politiloven) av 4. august 1995 nr. 53.

- Lov om styrking av menneskerettighetenes stilling i norsk rett (Menneskerettighetsloven) av 21. mai 1999 nr. 30.

- Lov om behandling av personopplysninger (Personopplysningsloven) av 14. april 2000 nr. 31.

- Lov om elektronisk kommunikasjon (Ekomloven) av 4. juli 2003 nr. 83.

Avgjørelser fra den Europeiske Menneskerettsdomstol (EMD):

- Sunday Times vs. The United Kingdom (1979). 2 EHRR 245.

- Malone vs. The United Kingdom (1984). Saksnr. 8691/79. 2.8.1984.

- Leander vs. Sweden (1987). Saksnr. 9248/81. 26.3.1987.

- Kruslin vs. France (1990). Saksnr. 11801/85. 24.4.1990.

- Botten vs. Norway (1996). Saksnr. 16206/90. 19.2.1996

- Walston vs. Norway (2003). Saksnr. 37372/97. 3.6.2003.

- Copland vs. The United Kingdom (2007). Saksnr. 62617/00. 3.4.2007.

Rettsavgjørelser – Lagmannsretten:

- RG. 2006 s. 811 (Lovdata online). Borgarting lagmannsrett – Kjennelse. 15.11.2005.

Rettsavgjørelser – Høyesterett:

- Rt. 1992 s. 904 (Lovdata online). Kjennelse. 23.6.1992.

- Rt. 1992 s. 898 (Lovdata online). Kjennelse. 19.6.1992.

- Rt. 1993 s. 1302 (Lovdata online). Kjennelse. 21.10.1993.

- Rt. 1997 s. 266 (Lovdata online). Kjennelse. 7.2.1997.

- Rt. 1997 s. 470 (Lovdata online). Kjennelse. 6.3.1997.

- Rt. 1999 s. 1944 (Lovdata online. Kjennelse. 20.12.1999.
- Rt. 1998 s. 309 (Lovdata online). Kjennelse. 9.2.1998.
- Rt. 1998 s. 1839 (Lovdata online). Kjennelse. 4.11.1998.
- Rt. 2000 s. 169 (Lovdata online). Kjennelse. 27.1.2000.
- Rt. 2005 s. 194 (Lovdata online). Kjennelse. 15.6.1995.
- Rt. 2009 s. 394 (Lovdata online). Kjennelse. Første kvartal 2008.
- Rt. 2009 s. 1011 (Lovdata online). Kjennelse. 26.8.2010.

Lovforarbeider:

- Innstilling om rettergangsmåten i straffesaker fra straffeprosesslovskomiteen. Avgitt juni 1969.
- **Ot.prp.nr. 2 (1985-1986)** – Om lov om endringer i bestemmelser i særlovgivningen om taushetsplikt (tilpassing til forvaltningsloven).
- **Ot.prp. nr. 36 (1994-1995)** – Lov om telekommunikasjon.
- **Ot.prp.nr. 31 (1997-1998)** – Endringslov til lov om telekommunikasjon.
- **Ot.prp.nr. 64 (1998-1999)** – Om lov om endringer i straffeprosessloven og straffeloven m.v.
- **Ot.prp.nr. 58 (2002-2003)** – Om lov om elektronisk kommunikasjon.
- **Ot.prp.nr. 40 (2004-2005)** – Om lov om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon av 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi.
- **NOU 1997:15** – ”Etterforskningsmetoder for bekjempelse av kriminalitet”.
- **NOU 1999:27** - ”Ytringsfrihed bør finde Sted”
- **NOU 2003:27** – ”Lovtiltak mot datakriminalitet”

- **NOU 2004:6** - ”Mellom effektivitet og personvern”
- **NOU 2009:1** – ”Individ og integritet”
- **NOU 2009:15** - ”Skjult informasjon – åpen kontroll”

Forskrifter:

- Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste av 16. februar 2004 nr. 401.

Internasjonale konvensjoner:

- Den Europeiske Menneskerettighetskonvensjonen (EMK) av 4. november 1950.
- Europarådets konvensjon av 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi.

Rapporter:

- **Post- og Teletilsynet**: *”Det norske markedet for elektroniske kommunikasjonstjenester 2009”*, 2010
- **Post- og Teletilsynet**: *”Personvern, taushetsplikt og elektronisk kommunikasjon”*, 2008.
- **Kontrollutvalget for kommunikasjonskontroll**: ”Årsrapport 2009”, Oslo, 21.4.2010

7 VEDLEGG

1. Kundeskjema fra Telenor Mobil.
2. Kundeskjema fra Tele 2.
3. Post- og Teletilsynets skjema om fritak for taushetsplikt.